

Ekwan E. Rhow - State Bar No. 174604
Dorothy Wolpert - State Bar No. 73213
Thomas R. Freeman - State Bar No. 135392
Marc E. Masters - State Bar No. 208375
mmasters@birdmarella.com
BIRD, MARELLA, BOXER, WOLPERT, NESSIM,
DROOKS, LINCENBERG & RHOW, P.C.
1875 Century Park East, 23rd Floor
Los Angeles, California 90067-2561
Telephone: (310) 201-2100
Facsimile: (310) 201-2110

*Attorneys for Plaintiffs Misty Hong, minor
A.S., through her mother and legal guardian
Laurel Slothower, and minor A.R., through
her mother and legal guardian Gilda Avila*

[Additional Counsel on Signature Page]

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

MISTY HONG, minor A.S., through her
mother and legal guardian LAUREL
SLOTHOWER, minor A.R., through her
mother and legal guardian GILDA AVILA,
MEGHAN SMITH, minors C.W. and I.W.,
through their mother and legal guardian
MIKHAILA WOODALL, and minor R.P.,
through her mother and legal guardian
LYNN PAVALON individually and on
behalf of all others similarly situated,

Plaintiffs,

vs.

BYTEDANCE, INC., a corporation,
TIKTOK, INC., a corporation; BEIJING
BYTEDANCE TECHNOLOGY CO.
LTD., a privately-held company; and
MUSICAL.LY, a corporation.

Defendants.

CASE NO. 5:19-cv-07792-LHK

Hon. Lucy H. Koh

**FIRST AMENDED CLASS ACTION
COMPLAINT FOR:**

- (1) Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030**
- (2) Violation of the California Comprehensive Data Access and Fraud Act, Cal. Pen. C. § 502**
- (3) Violation of the Right to Privacy - California Constitution**
- (4) Intrusion upon Seclusion**
- (5) Violation of the California Unfair Competition Law, Bus. & Prof. C. §§ 17200 et seq.**
- (6) Violation of the California False Advertising Law, Bus. & Prof. C. §§ 17500 et seq.**
- (7) Negligence**
- (8) Restitution / Unjust Enrichment**
- (9) Violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, et seq.**

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
II.	THE PARTIES.	1
A.	The Plaintiffs.	1
B.	The Defendants.....	2
C.	Alter Ego And Single Enterprise Allegations.	3
III.	JURISDICTION AND VENUE.....	6
IV.	THE RISE OF DEFENDANTS AND THEIR DANGEROUS APPS.	7
A.	Defendant Beijing ByteDance Becomes A China-Based Tech Giant Focused On Overseas Markets, Particularly In The United States.....	7
B.	The Musical.ly App Evolves Into The TikTok App.	8
C.	The TikTok App Becomes A Global Phenomenon With A Strong Presence In The United States.	9
V.	DEFENDANTS’ THEFT OF PRIVATE AND PERSONALLY-IDENTIFIABLE TIKTOK USER DATA AND CONTENT.....	12
A.	Defendants’ Secret Taking Of Private TikTok User Videos and TikTok User/Device Identifiers Without Notice Or Consent.	12
1.	Defendants Settle An FTC Lawsuit Alleging They Unlawfully Collected And Used Children’s Data.	12
2.	The TikTok App Secretly Takes Users’ Private Videos Before Users Are Given The Choice Whether To Save Or Post Them.	12
3.	The TikTok App Covertly Takes User/Device Identifiers.....	14
4.	Defendants’ Theft Of Private And Personally-Identifiable User Data And Content Begins Even Before Users Can Choose Whether To Sign Up With TikTok And Create An Account.	16
5.	Defendants’ Theft Of Private And Personally-Identifiable Data And Content Continues Even After Users Close The TikTok App.....	17
6.	Defendants Carefully Conceal Their Misconduct.....	17
7.	Defendants’ Privacy Policies And Terms Of Use Do Not Constitute Notice Of, Nor Consent To, TikTok User Data Theft, The Arbitration Provision Or The Class Action Waiver.....	17
B.	Defendants Come Under United States Government Scrutiny.	19

1	1.	The United States Government Investigates Defendants’ Stockpiling Of TikTok Users’ Private And Personally-Identifiable Data And Content For The Chinese Government.....	19
2			
3	2.	Defendants Unpersuasively Deny They Transfer TikTok Users’ Private And Personally-Identifiable Data And Content To The Chinese Government.	21
4			
5	C.	Transfers Of Private And Personally-Identifiable User Data And Content From TikTok Users To China Without Notice Or Consent.	22
6			
7	1.	The TikTok App Secretly Transfers Private And Personally-Identifiable User Data And Content To Servers In China.	22
8			
9	2.	Defendants’ Privacy Policies Do Not Constitute Notice Of Or Consent To The Transfer Of Private And Personally-Identifiable TikTok User Data And Content To Servers In China.	25
10			
11	3.	The China-Based Tech Giants Also Possess TikTok Users’ Private And Personally-Identifiable Data And Content While They Work Cooperatively With The Chinese Government.	25
12	VI.	DEFENDANTS’ THEFT OF TIKTOK USER BIOMETRICS.....	30
13	A.	The Illinois Biometric Information Privacy Act Regulates Face Geometry Scans, Voiceprints And Information Derived Therefrom.	30
14			
15	B.	Defendants Unlawfully Collect, Use And Profit From TikTok User Biometrics, Face Geometry Scans, Voiceprints And Information Derived Therefrom.	31
16			
17	1.	Defendants’ BIPA And Other Biometrics-Related Violations Are Evidenced By The TikTok App’s Functionality And Code.....	32
18			
19	2.	Defendants’ BIPA And Other Biometrics-Related Violations Are Further Evidenced By Defendants’ China-Based Operations.....	37
20			
21	3.	Defendants’ BIPA And Other Biometrics-Related Violations Are Also Evidenced By Their Obligation To Accumulate And Share Data, Including Biometrics, With The Chinese Government.....	43
22	VII.	DEFENDANTS UNJUSTLY PROFIT WHILE PLAINTIFFS, THE CLASS AND THE TWO SUBCLASSES SUFFER HARM.....	50
23	VIII.	FRAUDULENT CONCEALMENT AND TOLLING.	51
24	IX.	NAMED PLAINTIFF ALLEGATIONS.....	52
25	A.	The California Plaintiffs.....	52
26			
27	1.	Plaintiff Misty Hong.....	52
28			
	2.	Plaintiff A.S.....	53
	3.	Plaintiff A.R.	55

1	B.	The Illinois Plaintiffs.....	57
2	1.	Plaintiff Meghan Smith.	57
3	2.	Plaintiffs C.W. and I.W.....	58
4	3.	Plaintiff R.P.	60
5	X.	CLASS ALLEGATIONS.....	61
6	XI.	CAUSES OF ACTION.....	66
7	XII.	PRAYER FOR RELIEF.	86
8	XIII.	DEMAND FOR JURY TRIAL.	88

1 **I. INTRODUCTION.**

2 1. TikTok is one of the most popular entertainment apps for mobile devices in
3 the United States. It has acquired one of the largest installed user bases in the country on
4 the strength of its popular 15-second videos of fun activities like dancing, lip-syncing, and
5 stunts. Unknown to its users, however, the TikTok app also includes China-based
6 surveillance software. The TikTok app clandestinely has vacuumed up and transferred to
7 servers in China (and to other servers accessible from within China) vast quantities of
8 private and personally-identifiable user data and content that can be employed to identify,
9 profile and track the physical and digital location and activities of United States users now
10 and in the future.

11 2. The TikTok app also surreptitiously has taken TikTok users' private draft
12 videos they never intended for publication – without notice or consent. Defendants and
13 their sophisticated China-based engineering team covertly mine these private videos, as
14 well as publicly posted TikTok user videos, for highly sensitive and immutable biometric
15 identifiers and information. In addition to this mining of TikTok user videos at the server
16 level in China, the functionality and code of the TikTok app itself evidences Defendants'
17 collection and use of TikTok users' biometric identifiers and information – again without
18 notice or consent.

19 3. In short, the TikTok app's lighthearted fun comes at a heavy cost.
20 Meanwhile, Defendants unjustly profit from the secret harvesting of this massive array of
21 private and personally-identifiable TikTok user data and content by using it for targeted
22 advertising, improvements to Defendants' artificial intelligence technologies, the filing of
23 patent applications, and the development of consumer demand for, and use of, Defendants'
24 other products. Defendants' conduct violates statutory, constitutional, and common law
25 privacy, data, biometrics and consumer protections, and it should be stopped.

26 **II. THE PARTIES.**

27 **A. The Plaintiffs.**

28 4. Plaintiff Misty Hong is, and at all relevant times was, an individual and

1 resident of Palo Alto, California.

2 5. Plaintiff A.S., a minor, is, and at all relevant times was, an individual and
3 resident of Stevenson Ranch, California. A.S. brings this suit by and through her mother
4 and legal guardian, Laurel Slothower, who is, and at all relevant times was, an individual
5 and resident of Stevenson Ranch, California.

6 6. Plaintiff A.R., a minor, is, and at all relevant times was, an individual and
7 resident of Pasadena, California. A.R. brings this suit by and through her mother and legal
8 guardian, Gilda Avila, who is, and at all relevant times was, an individual and resident of
9 Pasadena, California.¹

10 7. Plaintiff Meghan Smith is, and at all relevant times was, an individual and
11 resident of Champagne, Illinois.

12 8. Plaintiffs C.W., a minor, and I.W., a minor, are, and at all relevant times
13 were, individuals and residents of Chicago, Illinois. C.W. and I.W. bring this suit by and
14 through their mother and legal guardian, Mikhaila Woodall, who is, and at all relevant
15 times was, an individual and resident of Chicago, Illinois.

16 9. Plaintiff R.P., a minor, is, and at all relevant times was, an individual and
17 resident of Chicago, Illinois. R.P. brings this suit by and through her mother and legal
18 guardian, Lynn Pavalon, who is, and at all relevant times was, an individual and resident of
19 Chicago, Illinois.²

20 **B. The Defendants.**

21 10. Defendant ByteDance, Inc. is, and at all relevant times was, a Delaware
22 corporation with its principal place of business in Palo Alto, California. Defendant
23 ByteDance, Inc. is a wholly-owned subsidiary of ByteDance, Ltd., a Cayman Islands
24 corporation.

25 _____
26 ¹ Plaintiffs Misty Hong, A.S. and A.R. are collectively referred to as the “California Plaintiffs.”

27 ² Plaintiffs Meghan Smith, C.W., I.W. and R.P. are collectively referred to as the “Illinois
28 Plaintiffs.” The California Plaintiffs and the Illinois Plaintiffs are collectively referred to as the
“Plaintiffs.”

11. Defendant TikTok, Inc. f/k/a Musical.ly, Inc. (“TikTok, Inc.”) is, and at all relevant times was, a California corporation with its principal place of business in Culver City, California.³ Defendant TikTok, Inc. also maintains offices in Palo Alto, California and Mountain View, California.⁴ The name change from Musical.ly, Inc. to TikTok, Inc. occurred in May 2019. Defendant TikTok, Inc. is a wholly-owned subsidiary of TikTok, LLC, which in turn is a wholly-owned subsidiary of TikTok, Ltd. And TikTok, Ltd. – like Defendant ByteDance, Inc. – is a wholly owned subsidiary of ByteDance, Ltd.

12. Defendant Musical.ly n/k/a TikTok, Ltd. is, and at all relevant times was, a Cayman Island corporation with its principal place of business in Shanghai, China. Defendant Musical.ly was the parent company of Musical.ly, Inc. Defendant Musical.ly changed its name to TikTok, Ltd. and, as noted above, is a wholly-owned subsidiary of ByteDance, Ltd.

13. Defendant Beijing ByteDance Technology Co. Ltd. (“Beijing ByteDance”) is, and at all relevant times was, a privately held company headquartered in Beijing, China. Defendant Beijing ByteDance is a wholly-owned subsidiary of ByteDance Co., Ltd., which is also headquartered in Beijing, China. ByteDance Co., Ltd. is owned by founder Zhang Yiming (98.8%) and Zhang Lidong (1.2%). Defendant Beijing ByteDance and ByteDance Co., Ltd. operate as one company.

14. ByteDance, Ltd. owns 100% of ByteDance (HK) Co., Ltd., which is headquartered in Hong Kong. ByteDance (HK) Co., Ltd. in turn owns 100% of Beijing ByteDance Network Technology Co., Ltd., which is headquartered in Beijing, China.

C. Alter Ego And Single Enterprise Allegations.

15. At all relevant times, Defendants TikTok, Inc. and ByteDance, Inc. have

³ <https://www.cnbc.com/2019/10/14/tiktok-has-mountain-view-office-near-facebook-poaching-employees.html>.

⁴ <https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/>;
<https://www.cnbc.com/2019/10/14/tiktok-has-mountain-view-office-near-facebook-poaching-employees.html>.

1 shared offices in Silicon Valley⁵ and also have shared employees. U.S. and China-based
2 employees of the ByteDance family of companies perform work on and concerning the
3 TikTok app that is at the center of this lawsuit, including the functionality and operation of
4 the TikTok app and the Chinese version of the app (“Douyin”) that Defendant Beijing
5 ByteDance operates in China. One Director of Engineering in the Mountain View office
6 leads an “augmented reality” team that is tasked with transforming state-of-the-art artificial
7 intelligence and augmented reality technologies into fun features and creative tools for
8 both the TikTok and Douyin apps.

9 16. At all relevant times, Defendant Beijing ByteDance has directed the
10 operations of Defendants TikTok, Inc. and ByteDance, Inc. with respect to the TikTok app,
11 and Defendants TikTok, Inc. and ByteDance, Inc. have reported to Defendant Beijing
12 ByteDance. In fact, at all relevant times, Defendant Beijing ByteDance has collected and
13 analyzed data from the United States regarding the performance of various features of the
14 TikTok app, and has worked with Defendants TikTok, Inc. and Defendant ByteDance, Inc.
15 to address performance issues. Additionally, at all relevant times, Defendant Beijing
16 ByteDance and its engineers have done significant coding for the TikTok app and its many
17 versions and updates.

18 17. At certain relevant times, with respect to Defendants’ monitoring and
19 censorship of content on the TikTok app, management in China has determined content
20 review policies enforced in Defendant TikTok, Inc.’s Culver City office; a content review
21 manager in the same Culver City office was reporting to someone in China; and another
22 content reviewer was required to seek authorization from someone in China in order to
23 access non-published information about user accounts when content concerns arose. Also,
24 at certain relevant times Defendant Beijing ByteDance employed a vast number of content
25 reviewers in China to review TikTok videos uploaded by United States users, and these

26
27 ⁵ In addition to ByteDance-TikTok cross-listed personnel in Palo Alto, TikTok logos and
28 paraphernalia are found in the ByteDance, Inc. Palo Alto office. *See*
<https://www.youtube.com/watch?v=RymGJG0miv0>.

1 reviewers in China had authority to take down any such videos if the content was deemed
2 inappropriate or illegal.

3 18. These facts are consistent with public reporting. For example, “[m]ultiple
4 TikTok sources, who spoke with *The Intercept* on the condition of anonymity ...,
5 emphasized the primacy of ByteDance’s Beijing HQ over the global TikTok operation,
6 explaining that their ever-shifting decisions about what’s censored and what’s boosted
7 are dictated by Chinese staff, whose policy declarations are then filtered around
8 TikTok’s 12 global offices, translated into rough English, finally settling into a muddle
9 of Beijing authoritarianism crossed with the usual Silicon Valley prudishness.”⁶

10 19. At certain relevant times, Defendant Beijing ByteDance employees have
11 collected TikTok users’ feedback regarding upgraded and/or newly-introduced features,
12 and the departments responsible for managing and monitoring TikTok user experience
13 have been based in China. At certain relevant times, employees in these departments
14 reported to their supervisors in China, who in turn shared their findings with Defendant
15 TikTok, Inc. in the United States. At certain relevant times, Defendant Beijing ByteDance
16 employees also distributed questionnaires to TikTok users, and collected and recorded
17 reports from such users about problems they were experiencing. At certain relevant times,
18 employees in the United States contacted TikTok users, and took notes regarding such
19 users’ experiences. At certain relevant times, these notes were translated into Chinese and
20 sent to Defendant Beijing ByteDance executives to review and analyze.

21 20. At certain relevant times, Defendant Beijing ByteDance made key strategy
22 decisions for Defendants TikTok, Inc. and ByteDance, Inc., as well as for offices
23 elsewhere in the world, and Defendants TikTok, Inc., ByteDance, Inc. and the other offices
24 were tasked with executing such decisions. A publicly-available interview of Isaac Bess
25 and Gregory Justice on YouTube is consistent with these facts. In that interview, Isaac
26 Bess identifies himself as responsible for leading “ByteDance” business development from

27 _____
28 ⁶ <https://theintercept.com/2020/03/16/tiktok-app-moderators-users-discrimination/>.

1 Los Angeles, and Gregory Justice identifies himself as part of Defendant TikTok, Inc.’s
 2 content team in Los Angeles. Both discuss having regular all-hands bi-monthly meetings
 3 with the CEO in China to discuss global strategy with the “local teams.”⁷

4 21. At all relevant times, and in connection with the matters alleged herein, each
 5 Defendant acted as an agent, servant, partner, joint venturer and/or alter ego of each of the
 6 other Defendants, and acted in the course and scope of such agency, partnership, and
 7 relationship and/or in furtherance of such joint venture. Each Defendant acted with the
 8 knowledge and consent of each of the other Defendants and/or directed, authorized,
 9 affirmed, consented to, ratified, encouraged, approved, adopted, and/or participated in the
 10 acts or transactions of the other Defendants.

11 22. At all relevant times, and in connection with the matters alleged herein,
 12 Defendants were controlled and largely-owned by the same person, founder Zhang
 13 Yiming, and constitute a single enterprise with a unity of interest. Recognition of the
 14 privilege of separate existence under such circumstances would promote injustice.

15 **III. JURISDICTION AND VENUE.**

16 23. This Court has subject matter jurisdiction over this action pursuant to 28
 17 U.S.C. § 1332(d) & 1367 because: (i) this is a class action in which the matter in
 18 controversy exceeds the sum of \$5,000,000, exclusive of interest and costs; (ii) there are
 19 100 or more class members; and (iii) some members of the class are citizens of states
 20 different from some Defendants, and also because two Defendants are citizens or subjects
 21 of a foreign state.

22 24. This Court has personal jurisdiction over Defendants because: (i) they
 23 transact business in the United States, including in this District; (ii) they have substantial
 24 aggregate contacts with the United States, including in this District; (iii) they engaged and
 25 are engaging in conduct that has and had a direct, substantial, reasonably foreseeable, and
 26 intended effect of causing injury to persons throughout the United States, including in this
 27 _____

28 ⁷ <https://www.youtube.com/watch?v=IKV6wsdI4-A> (at 0:20 – 0:54; 15:59 – 17:08).

District, and purposely availed themselves of the laws of the United States.

25. In accordance with 28 U.S.C. § 1391, venue is proper in this District because: (i) a substantial part of the conduct giving rise to the claims occurred in and/or emanated from this District; (ii) Defendants transact business in this District; (iii) one Defendant has its principal place of business in this District; (iv) two Defendants have offices in this District; and (v) Plaintiff Misty Hong resides in this District.

IV. THE RISE OF DEFENDANTS AND THEIR DANGEROUS APPS.

A. Defendant Beijing ByteDance Becomes A China-Based Tech Giant Focused On Overseas Markets, Particularly In The United States.

26. Defendant Beijing ByteDance was founded in 2012 and makes a variety of video and news-aggregation apps.⁸ It “regards its platforms as part of an artificial intelligence company powered by algorithms that ‘learn’ each user’s interests and preferences through repeat interaction.”⁹ Because Defendant Beijing ByteDance emerged only after other China-based tech giants had taken over the market in China, Defendant Beijing ByteDance has looked to overseas markets, including those in the United States, for growth.¹⁰

27. Defendant Beijing ByteDance had \$7.2 billion in annual revenue for the year 2018. It far surpassed this number in 2019, booking \$7 billion to \$8.4 billion in revenue in a better-than-expected result for the first half of 2019.¹¹ Defendant Beijing ByteDance currently is worth between \$75 billion and \$78 billion.¹² Investors in Defendant Beijing

⁸ <https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-is-serious-11561780861>.

⁹ <https://www.law360.com/articles/1213180/sens-want-tiktok-investigated-for-national-security-threats>; https://www.cotton.senate.gov/?p=press_release&id=1239.

¹⁰ <https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-is-serious-11561780861>.

¹¹ <https://www.cnbc.com/2019/09/30/tiktok-owner-bytedances-first-half-revenue-better-than-expected-at-over-7-billion-sources.html>.

¹² <https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us->

ByteDance include Sequoia Capital China, Russian billionaire Yuri Milner, Japanese technology giant SoftBank, and big private-equity firms such as KKR, General Atlantic, and Hillhouse Capital Group.¹³

28. Most of Defendant Beijing ByteDance’s revenue is generated from advertising.¹⁴ “ByteDance has [] been doubling down on its advertising business as the company’s management sets increasingly ambitious revenue goals.”¹⁵ “As with pretty much all major social media and content startups, ByteDance monetises through advertising. Specifically, it runs targeted advertising within user feeds – providing them promotional content in between using the app.”¹⁶

B. The Musical.ly App Evolves Into The TikTok App.

29. Defendant Musical.ly (named, and now known as, TikTok, Ltd.) and Defendant Musical.ly, Inc. (named, and now known as, TikTok, Inc.) launched the highly-popular social media and social networking app “Muscial.ly” in 2014. This app allows its users to (i) create video selfies of themselves dancing and/or lip-syncing with a musical soundtrack in the background, and (ii) share such videos with friends.¹⁷ There are simple tools provided by the Musical.ly app that users can utilize to create and edit these videos, and the app provides a large online music library from which users may select their background music. The Musical.ly app was designed “to capture the YouTube phenomenon of teenagers sharing videos of themselves singing or dancing to popular

[views-about-censorship-often-were-overridden-by-chinese-bosses/](https://www.reuters.com/article/us-tiktok-cfius-exclusive/exclusive-us-opens-national-security-investigation-into-tiktok-sources-idUSKBN1XB4IL);

<https://www.reuters.com/article/us-tiktok-cfius-exclusive/exclusive-us-opens-national-security-investigation-into-tiktok-sources-idUSKBN1XB4IL>.

¹³ <https://www.wsj.com/articles/lip-syncing-app-musical-ly-is-acquired-for-as-much-as-1-billion-1510278123>; <https://www.reuters.com/article/us-tiktok-cfius-exclusive/exclusive-us-opens-national-security-investigation-into-tiktok-sources-idUSKBN1XB4IL>.

¹⁴ <https://www.bloomberg.com/news/articles/2019-01-15/bytedance-is-said-to-hit-lower-end-of-sales-goal-amid-slowdown>.

¹⁵ <https://technode.com/2019/09/20/bytedance-launches-video-ad-tools-for-tiktok-douyin/>.

¹⁶ <https://www.businessofapps.com/insights/bytedance-social-media-advertising-company/>.

¹⁷ <https://www.wsj.com/articles/lip-syncing-app-musical-ly-is-acquired-for-as-much-as-1-billion-1510278123>.

1 music.”¹⁸ Beyond the creation and sharing of videos, the Musical.ly app provides a
 2 platform through which users can interact, including by commenting on other users’ videos
 3 and “following” other users’ accounts. Users also can send direct messages in order to
 4 communicate with other users on the app. By November 2017, the Musical.ly app had 60
 5 million monthly active users.¹⁹

6 30. Meanwhile, in 2016, Defendant Beijing ByteDance launched its own app
 7 called “Douyin” in China, which mimicked the Musical.ly app.²⁰ By 2017, shortly before
 8 its purchase of Defendants Musical.ly and Musical.ly, Inc., Defendant Beijing ByteDance
 9 introduced an English-language version of the Douyin app outside China under the name
 10 “TikTok.” In August 2018, after having acquired Defendants Musical.ly and Musical.ly,
 11 Inc., Defendant Beijing ByteDance combined the Musical.ly app with its TikTok app,
 12 merging all existing accounts and data into a single app under the retained “TikTok”
 13 name.²¹

14 31. The Musical.ly and TikTok apps are hereafter collectively referred to as the
 15 “TikTok app,” and the Musical.ly and TikTok users are hereafter collectively referred to as
 16 the “TikTok users.”

17 **C. The TikTok App Becomes A Global Phenomenon With A Strong**
 18 **Presence In The United States.**

19 32. The TikTok app has become “one of the world’s fastest-growing social
 20 media platforms” and a “global phenomenon” with a massive American audience.²² In
 21

22 ¹⁸ <https://www.wsj.com/articles/lip-syncing-app-musical-ly-is-acquired-for-as-much-as-1-billion-1510278123>.
 23

24 ¹⁹ <https://www.wsj.com/articles/lip-syncing-app-musical-ly-is-acquired-for-as-much-as-1-billion-1510278123>; <https://www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html>.
 25

26 ²⁰ <https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-is-serious-11561780861>.
 27

28 ²¹ <http://culture.affinitymagazine.us/tik-tok-is-scamming-people-stealing-information/>.

²² <https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us->

1 November 2019, the *Washington Post* reported that the TikTok app had been downloaded
 2 more than 1.3 billion times worldwide, and more than 120 million times in the United
 3 States.²³ However, by April 2020, *TechCrunch* reported that the TikTok app’s worldwide
 4 downloads already had surpassed 2 billion, and that in “the quarter that ended on March 31,
 5 TikTok was downloaded 315 million times — the highest number of downloads for any app
 6 in a quarter.”²⁴ It is the most downloaded non-game app in the world.²⁵ The TikTok app
 7 routinely outranks its top competitors – such as Facebook, Snapchat, and Instagram – on
 8 the Apple and Google app stores.²⁶ In fact, it has been the most downloaded app on the
 9 Apple and Google app stores for months.²⁷ As of August 2019, the TikTok and Douyin
 10 apps had 625 million monthly active users.²⁸ The average user opened the TikTok app
 11 more than 8 times per day and spent approximately 45 minutes on the app daily as of
 12 March 2019.²⁹

13 33. In January 2020, *Barron’s* reported on the TikTok app’s revenue: “The
 14 wildly popular short-video service generated \$176.9 million in revenue in 2019—71% of
 15 the total \$247.6 million in revenue the app has ever generated, according to new data from
 16 the app-tracking firm SensorTower. In the fourth quarter alone, TikTok had revenue of
 17 \$88.5 million, up two times from the third quarter and up six times year over year, most of
 18 that from advertising and in-app purchases, SensorTower reports. China accounted for

19 [views-about-censorship-often-were-overridden-by-chinese-bosses/](#).

20 ²³ <https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/>.

21 ²⁴ <https://techcrunch.com/2020/04/29/tiktok-tops-2-billion-downloads/>.

22 ²⁵ <https://www.cnbc.com/2019/07/25/china-camera-apps-may-open-up-user-data-to-beijing-government-requests.html>.

23 ²⁶ <https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/>.

24 ²⁷ <https://thehill.com/policy/technology/469114-tiktok-faces-lawmaker-anger-over-china-ties>.

25 ²⁸ <https://thehill.com/policy/technology/469114-tiktok-faces-lawmaker-anger-over-china-ties>.

26 ²⁹ <https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-is-serious-11561780861>.

1 about 69% of the company’s 2019 revenue, according to the firm, with U.S. revenues
 2 accounting for 20%.”³⁰ Evidencing the TikTok app’s rapid growth, three months later,
 3 *TechCrunch* reported that: “Users have spent about \$456.7 million on TikTok to date, up
 4 from \$175 million five months ago. Much of this spending — about 72.3% — has happened
 5 in China. Users in the United States have spent about \$86.5 million on the app, making the
 6 nation the second most important market for TikTok from the revenue standpoint.”³¹

7 34. This level of success globally and in the United States is rare for a China-
 8 based tech giant. Facebook CEO Mark Zuckerberg acknowledged as much, stating that the
 9 TikTok app “is really the first consumer internet product built by one of the Chinese tech
 10 giants that is doing quite well around the world. It’s starting to do well in the U.S.,
 11 especially with young folks.”³² Indeed, Defendant TikTok, Inc. recently took over office
 12 space in Silicon Valley once occupied by Facebook’s WhatsApp messaging app, and is
 13 poaching employees from rival Facebook by offering salaries as much as 20% higher.³³
 14 Other competitors from whom Defendant TikTok, Inc. is hiring away employees include
 15 Snap, Hulu, Apple, YouTube and Amazon.³⁴

16 35. One key to Defendants’ financial success is the targeted advertising that they
 17 run through the TikTok app. Such targeted advertising relies heavily upon knowledge of
 18 each user’s preferences.³⁵ Through a secretive and highly-invasive information gathering
 19 campaign, Defendants have unlawfully accumulated private and personally-identifiable
 20 data and content on TikTok users that Defendants are assembling in user profiles or

21
 22 ³⁰ <https://www.barrons.com/articles/beware-facebook-tiktok-revenues-are-exploding-51579201752>.

23 ³¹ <https://techcrunch.com/2020/04/29/tiktok-tops-2-billion-downloads/>.

24 ³² <https://www.cnbc.com/2019/10/14/tiktok-has-mountain-view-office-near-facebook-poaching-employees.html>.

25 ³³ <https://www.cnbc.com/2019/10/14/tiktok-has-mountain-view-office-near-facebook-poaching-employees.html>.

26 ³⁴ <https://www.cnbc.com/2019/10/14/tiktok-has-mountain-view-office-near-facebook-poaching-employees.html>.

27 ³⁵ <https://www.digitaltrends.com/social-media/tiktok-advertiser-audience-network-targeted-ads/>.

dossiers and monetizing for the purpose of unjustly profiting from their unlawful activities.

V. DEFENDANTS' THEFT OF PRIVATE AND PERSONALLY-IDENTIFIABLE TIKTOK USER DATA AND CONTENT.

A. Defendants' Secret Taking Of Private TikTok User Videos and TikTok User/Device Identifiers Without Notice Or Consent.

1. Defendants Settle An FTC Lawsuit Alleging They Unlawfully Collected And Used Children's Data.

36. On February 27, 2019, the United States, on behalf of the Federal Trade Commission ("FTC"), filed a lawsuit against Defendants Musical.ly and Musical.ly, Inc. alleging they had violated the Children's Online Privacy Protection Act by collecting and using personal data from children under age 13 without the required notice and consent.³⁶

37. On the same date, Defendants Musical.ly and Musical.ly, Inc. stipulated to an order mandating, among other things, a civil penalty in the amount of \$5.7 million and injunctive relief concerning the collection and destruction of children's personal data.³⁷

38. This is the largest civil penalty ever imposed for such a violation.³⁸ The FTC also published a statement indicating that, "[i]n our view, these practices reflected the company's willingness to pursue growth even at the expense of endangering children."³⁹

2. The TikTok App Secretly Takes Users' Private Videos Before Users Are Given The Choice Whether To Save Or Post Them.

39. Unless shared through the affirmative consent of the TikTok user, videos created using the TikTok app, which often include close-ups of faces and private acts

³⁶ *United States of America v. Musical.ly and Musical.ly, Inc.*, United States District Court, Central District of California, Case No. 2:19-cv-1439.

³⁷ *United States of America v. Musical.ly and Musical.ly, Inc.*, United States District Court, Central District of California, Case No. 2:19-cv-1439.

³⁸ <https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-is-serious-11561780861>; <https://www.techinasia.com/tiktok-owner-bytedance-gathers-1-billion-monthly-active-users-apps>.

³⁹ <https://www.nbcnews.com/tech/tech-news/tiktok-pay-5-7-million-over-alleged-violation-child-privacy-n977186>.

1 unintended for public consumption, are inherently private, personal and sensitive.

2 40. After using the TikTok app to record a video, a screen presents TikTok users
3 with certain options, including the following: (i) an “x” button; (ii) a “next” button; and
4 (iii) a button for effects. The “x” button takes TikTok users to a screen with options,
5 including “reshoot” and “exit.” The “next” button takes TikTok users to a screen with
6 options, including “save” and “post.” The “effects” button takes TikTok users to a screen
7 offering the ability to modify the video.

8 41. Once TikTok users click the “next” button, but before they click either the
9 “save” or “post” buttons, their *private videos that are neither saved nor posted* (the
10 “Private Videos”) are transferred from their mobile devices to the following domain owned
11 and controlled by Defendants: muscdn.com. The “mus” portion of the domain name stands
12 for Musical.ly, and the “cdn” portion of the domain name stands for content distribution
13 network.

14 42. During the secret transfer of TikTok users’ Private Videos to the domain and
15 servers mentioned above, there is no progress bar or any other indication that their Private
16 Videos are being transferred. Nor is the taking of the Private Videos disclosed in any of
17 Defendants’ privacy policies or other disclosure documentation. TikTok users are thus
18 prevented from knowing that Defendants have taken their Private Videos. No user consent
19 exists.

20 43. This highly invasive breach of TikTok users’ privacy is not the only harm
21 that befalls such users as a result of Defendants’ theft of their Private Videos. Defendants
22 also take highly sensitive and immutable biometric identifiers and information from these
23 Private Videos, as discussed below, and unjustly profit from such activities.

24 44. Defendants released a December 2019 version of the TikTok app that
25 transfers five thumbnail images uniformly distributed across each of the Private Videos
26 (the “Private Video Images”) to byteoversea.net. The domain byteoversea.net is controlled
27 by Defendants and has numerous sub-domains. Accordingly, when data and content
28 arrives at byteoversea.net, it is routed to one or more of these sub-domains. The various

1 sub-domains are spread across the globe, including within China.

2 45. Defendants' taking of the Private Video Images is not disclosed in any of
3 Defendants' privacy policies or other disclosure documentation. TikTok users are thus
4 prevented from knowing that Defendants have taken their Private Video Images. No user
5 consent exists.

6 **3. The TikTok App Covertly Takes User/Device Identifiers.**

7 46. Also unknown to TikTok users is that the seemingly innocuous TikTok app
8 infiltrates their mobile devices and extracts a remarkably broad array of private and
9 personally-identifiable data and content that Defendants use to track and profile TikTok
10 users for the purpose of, among other things, targeting them with advertisements from
11 which Defendants unjustly profit.

12 47. This unlawful secret taking of private and personally-identifiable data and
13 content from TikTok users' mobile devices is contrary to American norms. The United
14 States Supreme Court has recognized that, in contemporary society, cell phones are so
15 ubiquitous and inextricably intertwined with the user's personal privacy that such devices
16 have become "*almost a 'feature of human anatomy.'*" *Carpenter v. United States*, 138
17 S.Ct. 2206, 2218 (2018) (quoting *Riley v. California*, 573 U.S. 373, 385 (2014)). The
18 United States Constitution thus provides a privacy right that protects individuals against
19 unreasonable governmental searches of their physical movements through historical cell
20 phone records in the possession of their service providers. *Carpenter*, 138 S.Ct. at 2218.

21 48. From each mobile device on which the TikTok app is installed, Defendants
22 take a combination of, among other items, the following user identifiers and mobile device
23 identifiers ("User/Device Identifiers"):

- 24 a. username, password, age/birthday, email address, and profile image;
- 25 b. user-generated content, including messages sent through the apps;
- 26 c. phone and social network contacts;
- 27 d. the mobile device's WiFi MAC address (*i.e.*, media access control
- 28 address), which is the unique hardware number on the WiFi card adapter that tells the

1 internet who is connected to it;

2 e. the mobile device's International Mobile Equipment Identity
3 ("IMEI") number, which is a unique number given to every mobile device that is used to
4 route calls to one's phone, and that reflects information about the origin, model, and serial
5 number of the mobile device;

6 f. the user's International Mobile Subscriber Identity ("IMSI") number,
7 which is a unique number given to every subscriber to a mobile network;

8 g. the IP address (*i.e.*, Internet Protocol address), which is a numerical
9 label assigned to each user mobile device connected to a computer network that uses the
10 Internet Protocol for communication. IP addresses allow the location of literally billions of
11 digital devices that are connected to the Internet to be pinpointed and differentiated from
12 all other such devices;

13 h. the device ID, which is a unique, identifying number or group of
14 numbers assigned to the user's individual mobile device that is separate from the hardware
15 serial number;

16 i. the OS version, which is the operating system on the user's mobile
17 device;

18 j. the mobile device brand and model/version;

19 k. the hardware serial number, which is the unique, identifying number
20 or group of numbers assigned to the user's individual mobile device;

21 l. the Advertising ID, which is a unique ID for advertising that provides
22 developers with a simple, standard system to monetize their apps;

23 m. mobile carrier information (*e.g.*, the name of the phone company);

24 n. network information, including the technology that the carrier uses;

25 o. browsing history;

26 p. cookies;

27 q. metadata; and

28 r. precise physical location, including based on SIM card, cell towers

1 and/or GPS.

2 49. Theft of physical and digital location tracking data is highly invasive of
3 TikTok users' privacy rights. Two United States Senators observed that "[l]ocation data is
4 among the most sensitive personal information that a user can share with a company ...
5 Today, modern smartphones can reveal location data beyond a mere street address. The
6 technology is sophisticated enough to identify on which floor of a building the device is
7 located."⁴⁰ Location data reveals *private living patterns* of TikTok users, including where
8 they work, where they reside, where they go to school, and when they are at each of these
9 locations. Location data, either standing alone or combined with other information,
10 exposes deeply-private and personal information about TikTok users' *health, religion,*
11 *politics and intimate relationships.*

12 50. The TikTok app also invites users to sign in through Facebook, Google, and
13 Twitter. What users do not know is that this "single sign-on" option gives Defendants
14 access to TikTok users' private and personally-identifiable data and content stored on these
15 *other social media accounts*, including User/Device Identifiers such as the user's photos
16 and friends/contacts information.

17 **4. Defendants' Theft Of Private And Personally-Identifiable User**
18 **Data And Content Begins Even Before Users Can Choose**
19 **Whether To Sign Up With TikTok And Create An Account.**

20 51. The TikTok app begins taking private and personally identifiable user data
21 and content immediately upon the completion of the download process and before TikTok
22 users even have the opportunity to sign-up and create an account. TikTok users therefore
23 do not have an opportunity to learn about the existence of, much less consent to, any of
24 Defendants' privacy policies or other disclosure documentation before the TikTok app
25 begins mining their mobile devices for their data and content.

26
27

⁴⁰ <https://www.law360.com/consumerprotection/articles/1221312/sens-prod-zuckerberg-why-keep-tracking-user-locations->
28 [keep-tracking-user-locations-](https://www.law360.com/consumerprotection/articles/1221312/sens-prod-zuckerberg-why-keep-tracking-user-locations-).

1

2 **5. Defendants’ Theft Of Private And Personally-Identifiable Data**

3 **And Content Continues Even After Users Close The TikTok App.**

4 52. Even when TikTok users stop using the app and close it, Defendants

5 continue to harvest private and personally-identifiable data and content from such users’

6 mobile devices. There are no disclosures in any of Defendants’ privacy policies or other

7 disclosure documentation that such surreptitious taking of private and personally-

8 identifiable user data and content occurs when the TikTok app is closed. TikTok users are

9 thus prevented from knowing that Defendants have taken their private and personally-

10 identifiable data and content while the TikTok app is closed. No user consent exists.

11 **6. Defendants Carefully Conceal Their Misconduct.**

12 53. At the same time that Defendants utilize the TikTok app to covertly tap into

13 a massive array of private and personally-identifiable user data and content, they go to

14 great lengths to hide their tracks. They do so by obfuscating the source code that would

15 reveal the private and personally-identifiable user data and content actually taken from

16 users’ mobile devices.

17 **7. Defendants’ Privacy Policies And Terms Of Use Do Not**

18 **Constitute Notice Of, Nor Consent To, TikTok User Data Theft,**

19 **The Arbitration Provision Or The Class Action Waiver.**

20 54. Defendants have adopted various privacy policies and terms of use for the

21 TikTok app over the years. Certain privacy policies, revealed by investigation of counsel

22 but not seen in the ordinary course by users, purport to disclose that the TikTok app takes

23 certain (but not all) of the private and personally-identifiable user data and content above.

24 Certain terms of use, revealed by investigation of counsel but not seen in the ordinary

25 course by users, purport to require arbitration and class action waivers.

26 55. Because the TikTok app begins taking private and personally-identifiable

27 user data and content – including User/Device Identifiers – immediately upon the

28 completion of the download process, and before TikTok users are even presented with the

1 option of signing-up for and creating an account, TikTok users have no notice of, and
2 cannot consent to, the privacy policies and terms of use prior to such theft. Moreover,
3 because the TikTok app takes Private Videos and Private Video Images even if TikTok
4 users have not signed up for an account, TikTok users who have not signed up for an
5 account have no notice of, and cannot consent to, the privacy policies and terms of use
6 prior to such theft.

7 56. Moreover, even at the point at which TikTok users have the option to sign-up
8 and create an account, Defendants do not provide such users actual notice of privacy
9 policies or terms of use. Nor do Defendants present TikTok users with conspicuously-
10 located and designed hyperlinks to their privacy policies and terms of use, much less
11 conspicuous warnings accompanying such hyperlinks. The TikTok app thus allows users
12 to utilize it without ever placing them on actual or constructive notice of the privacy
13 policies and terms of use. This lack of actual or constructive notice deprives TikTok users
14 of the opportunity to accept or reject TikTok's privacy policies and terms of use, rendering
15 such documents unenforceable. *See, e.g., Colgate v. Juul Labs, Inc.*, 402 F.Supp.3d 728
16 (N.D. Cal. 2019); *Arena v. Intuit Inc.*, 2020 WL 1189849 (N.D. Cal. 2020).

17 57. Additionally, certain privacy policies and terms of use are ambiguous as to
18 what conduct they purport to cover. Such privacy policies and terms of use are also
19 substantively and procedurally unconscionable. The ambiguities render meaningless the
20 purported disclosures and requirements in the remainder of these documents, and the
21 substantive and procedural unconscionability render such documents unenforceable.

22 58. Moreover, even if TikTok users in California had knowingly accepted the
23 terms of use (which they did not), the purported waiver of the right to seek public
24 injunctive relief in a court of law is unenforceable under California law. *See, e.g., McGill*
25 *v. Citibank*, 2 Cal.5th 945 (2017); *Blair v. Rent-A-Center*, 928 F.3d 819 (9th Cir. 2019).

1 **B. Defendants Come Under United States Government Scrutiny.**

2 **1. The United States Government Investigates Defendants’**
 3 **Stockpiling Of TikTok Users’ Private And Personally-Identifiable**
 4 **Data And Content For The Chinese Government.**

5 59. United States Senators Charles Schumer and Tom Cotton sent an October
 6 2019 letter to the Acting Director of National Intelligence describing “national security”
 7 risks associated with the TikTok app. The Senators noted that there is evidence that
 8 Defendants may share private and personally-identifiable user data and content with the
 9 Chinese government:

10 TikTok’s terms of service and privacy policies describe how it collects data
 11 from its users and their devices, including user content and communications,
 12 IP address, location-related data, device identifiers, cookies, metadata, and
 13 other sensitive personal information. While the company has stated that
 14 TikTok does not operate in China and stores U.S. user data in the U.S.,
 15 ByteDance is still required to adhere to the laws of China.

16 Security experts have voiced concerns that China’s vague patchwork of
 17 intelligence, national security, and cybersecurity laws compel Chinese
 18 companies to support and cooperate with intelligence work controlled by the
 19 Chinese Communist Party. ... With over 110 million downloads in the U.S.
 20 alone, TikTok is a potential counterintelligence threat we cannot ignore.
 21 Given these concerns, we ask that the Intelligence Community conduct an
 22 assessment of the national security risks posed by TikTok ... and brief
 23 Congress on these findings.⁴¹

24 60. The Committee on Foreign Investment in the United States (“CFIUS”) is an
 25 inter-agency committee of the United States government that reviews the national security

26
 27 ⁴¹ [https://www.law360.com/articles/1213180/sens-want-tiktok-investigated-for-national-security-](https://www.law360.com/articles/1213180/sens-want-tiktok-investigated-for-national-security-threats)
 28 [threats; https://www.cotton.senate.gov/?p=press_release&id=1239.](https://www.cotton.senate.gov/?p=press_release&id=1239)

1 implications of foreign investments in United States companies or operations. Chaired by
 2 the United States Secretary of the Treasury, CFIUS includes representatives from 16
 3 United States departments and agencies, including the Defense, State, Commerce and
 4 Homeland Security departments. CFIUS is reviewing Defendant Beijing ByteDance's
 5 acquisition of Defendants Musical.ly and Musical.ly, Inc.⁴²

6 61. Additionally, the Senate Judiciary Subcommittee on Crime and Terrorism
 7 held a hearing in November 2019 that Defendant TikTok, Inc. declined to attend although
 8 it had been invited. The Chairman, Senator Josh Hawley, stated in opening remarks that:
 9 "TikTok should answer ... to the millions of Americans who use their product with no idea
 10 of its risks."⁴³ Chairman Hawley also told reporters that: "The idea that TikTok is not
 11 sharing data, is not taking direction from Beijing, that just does not appear to be true."⁴⁴

12 62. Indeed, the risk that Defendants send TikTok user data to the Chinese
 13 government is so great that the U.S. Army has banned the app on government-owned
 14 devices. That decision was based on concerns specific to Defendants and their close
 15 relationship to the Chinese government. The Army banned the TikTok app despite the fact
 16 that it had been using it for recruiting purposes until it realized the risk.⁴⁵ The U.S. Navy,
 17 Marines, Air Force and Coast Guard, as well as the Department of Defense and the
 18 Transportation Security Administration have likewise banned the TikTok app due to the
 19 risk that user data is being sent to China.⁴⁶

20
 21
 22
 23 ⁴² <https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/>.

24 ⁴³ <https://thehill.com/policy/technology/469114-tiktok-faces-lawmaker-anger-over-china-ties>.

25 ⁴⁴ <https://thehill.com/policy/technology/469114-tiktok-faces-lawmaker-anger-over-china-ties>.

26 ⁴⁵ <https://www.businessinsider.com/us-government-agencies-have-banned-tiktok-app-2020-2>

27 ⁴⁶ <https://www.businessinsider.com/us-government-agencies-have-banned-tiktok-app-2020-2#1-the-navy-banned-tiktok-from-government-devices-1>; <https://www.engadget.com/2020-01-04-nearly-whole-us-military-bans-tiktok.html>
 28

1 **2. Defendants Unpersuasively Deny They Transfer TikTok Users’**
 2 **Private And Personally-Identifiable Data And Content To The**
 3 **Chinese Government.**

4 63. In July 2019, amid growing scrutiny, Defendant TikTok, Inc. retained
 5 consultants who opined that there is “no indication” that the Chinese government accessed
 6 TikTok users’ data.⁴⁷ But the lead consultant admitted that the review and analysis was
 7 limited to a narrow and recent four-month period: “He added that in the analysis from July
 8 [2019] to October [2019], which included interviews with TikTok employees and a review
 9 of the app’s underlying computer code, his team found no way TikTok could send data to
 10 China during those months.”⁴⁸ And, the consultants did not address whether TikTok user
 11 data could be accessed from, as opposed to “sent to,” China.

12 64. Defendant TikTok, Inc. also issued a public statement in which it
 13 represented: “First, let’s talk about data privacy and security. We store all TikTok U.S.
 14 user data in the United States, with backup redundancy in Singapore. Our data centers are
 15 located entirely outside of China, and none of our data is subject to Chinese law.”⁴⁹

16 65. This public statement is carefully couched in the present tense and studiously
 17 avoids mention of past practices. In fact, the statement does not actually say that no private
 18 and personally-identifiable user data and content is transferred to China. Rather, it says
 19 that private and personally-identifiable user data and content is stored in the United States
 20 (but not necessarily exclusively in the United States) and that the current data centers are
 21 located outside China (but not whether these data centers transfer private and personally-
 22 identifiable user data to China or make it accessible there). Even Defendant TikTok, Inc.’s
 23 February 2019 Privacy Policy, which is not viewed by users in the ordinary course, states

24 _____
 25 ⁴⁷ <https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/>.

26 ⁴⁸ <https://www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html>.

27 ⁴⁹ <https://newsroom.tiktok.com/en-us/statement-on-tiktoks-content-moderation-and-data-security-practices>.
 28

1 that “[w]e may share your information with a parent, subsidiary, or other affiliate of our
2 corporate group.” Although this language is ambiguous, it apparently “means it would
3 include China-based ByteDance.”⁵⁰ Accordingly, Defendant TikTok, Inc.’s public
4 statement (above) and its February 2019 Privacy Policy are, at best, highly misleading.

5 **C. Transfers Of Private And Personally-Identifiable User Data And**
6 **Content From TikTok Users To China Without Notice Or Consent.**

7 **1. The TikTok App Secretly Transfers Private And Personally-**
8 **Identifiable User Data And Content To Servers In China.**

9 66. *Affinity* published an article entitled “TikTok is Scamming People & Stealing
10 Information.” Quoting from a pre-2019 TikTok privacy policy, the article reports that
11 “they store and process user data in United States of America, Singapore, Japan or to
12 China.”⁵¹ The article also reports that Defendant TikTok, Inc. is “offering personal
13 information to third parties and the Chinese government.”⁵²

14 67. *CNBC* published an article entitled “China’s globally popular camera apps
15 may open up user data to Beijing requests” in which it confirms that a TikTok privacy
16 policy from 2018 acknowledged transmission of private and personally-identifiable user
17 data and content to China: “TikTok’s 2018 privacy policy said the company can transfer
18 international users’ data to China, according to archived versions of that web page.”⁵³
19 Even Defendant TikTok, Inc.’s August 2018 Privacy Policy, which is not seen by users
20 and which by its own terms does not even apply to United States users, states: “We will
21 also share your information with any member or affiliate of our group, in China, for the
22 purposes set out above, to assist in the improvement or optimisation of the Platform, ...
23

24 ⁵⁰ [https://www.cnbc.com/2019/07/25/china-camera-apps-may-open-up-user-data-to-beijing-](https://www.cnbc.com/2019/07/25/china-camera-apps-may-open-up-user-data-to-beijing-government-requests.html)
25 [government-requests.html](https://www.cnbc.com/2019/07/25/china-camera-apps-may-open-up-user-data-to-beijing-government-requests.html).

26 ⁵¹ <http://culture.affinitymagazine.us/tik-tok-is-scamming-people-stealing-information/>.

27 ⁵² <http://culture.affinitymagazine.us/tik-tok-is-scamming-people-stealing-information/>.

28 ⁵³ [https://www.cnbc.com/2019/07/25/china-camera-apps-may-open-up-user-data-to-beijing-](https://www.cnbc.com/2019/07/25/china-camera-apps-may-open-up-user-data-to-beijing-government-requests.html)
[government-requests.html](https://www.cnbc.com/2019/07/25/china-camera-apps-may-open-up-user-data-to-beijing-government-requests.html).

1 increase user numbers, development, engineering and analysis of information or for our
2 internal business purposes”

3 68. *Quartz* published an article by David Carroll entitled “Is TikTok a Chinese
4 Cambridge Analytica data bomb waiting to explode?” Mr. Carroll is an associate professor
5 at the Parsons School of Design in New York, and in 2017 he sued Cambridge Analytica
6 in the United Kingdom. In his *Quartz* article, Mr. Carroll quoted from Defendant TikTok,
7 Inc.’s August 2018 Privacy Policy that reveals that private and personally-identifiable user
8 data and content is transferred to China.⁵⁴ Mr. Carroll further reported that, in emails
9 between him and Defendant TikTok, Inc. in March and April 2019, Defendant TikTok,
10 Inc. (i) confirmed that, at least prior to February 2019, U.S. TikTok user data may have
11 been processed in China; and (ii) provided confusing answers about what happened after
12 that, including that U.S. TikTok user data may have continued to be processed by systems
13 operated by “one of our China registered entities,” and may exist there in some form, even
14 where such user data is stored elsewhere.⁵⁵

15 69. The *New York Times* has reported that a source “said the American
16 government had evidence of the [TikTok] app sending data to China.”⁵⁶ That explains why
17 the Defense Department, Navy, Army, Marines, Air Force, Coast Guard and
18 Transportation Security Administration have taken the extraordinary step of prohibiting
19 their members from using the TikTok app on any government-issued devices, and have
20 advised that their children also remove the TikTok app from their devices.⁵⁷ United States
21 Senators also have proposed a bill banning federal employees from using the TikTok app
22 on government-issued phones because it “presents a major security risk.”⁵⁸

23
24 ⁵⁴ <https://qz.com/1613020/tiktok-might-be-a-chinese-cambridge-analytica-scale-privacy-threat/>.

25 ⁵⁵ <https://qz.com/1613020/tiktok-might-be-a-chinese-cambridge-analytica-scale-privacy-threat/>.

26 ⁵⁶ <https://www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html>.

27 ⁵⁷ <https://www.wsj.com/articles/u-s-military-bans-tiktok-over-ties-to-china-11578090613>.

28 ⁵⁸ <https://www.reuters.com/article/us-usa-china-tiktok/us-senators-seek-to-ban-federal-employees-from-using-tiktok-on-their-phones-idUSKBN20Z1E4>.

1 **a. Evidence Of Post-February 2019 Transfers.**

2 70. Even after Defendant TikTok, Inc. adopted its February 2019 Privacy Policy,
3 the TikTok app secretly transferred private and personally-identifiable user data and
4 content to China where, under Chinese law, it is subject to collection and use by the
5 Chinese government. Specifically, Defendants used the TikTok app to transfer private and
6 personally-identifiable user data and content to the following two servers in China as
7 recently as April 2019: (i) bugly.qq.com and (ii) umeng.com.

8 71. Private and personally-identifiable TikTok user data and content transferred
9 to bugly.qq.com as recently as April 2019 includes at least the following items: (i) the OS
10 version; (ii) the mobile device model; (iii) the WiFi MAC address; (iv) the hardware serial
11 number; (v) the device ID and (vi) the IP address. Private and personally-identifiable
12 TikTok user data and content transferred to umeng.com as recently as April 2019 includes
13 these same six items, plus at least the following item: (vii) the number of bytes users'
14 mobile devices have uploaded and downloaded.

15 **b. Evidence Of Pre-February 2019 Transfers.**

16 72. The TikTok app transferred private and personally-identifiable TikTok user
17 data and content to various servers in China prior to the February 2019 Privacy Policy,
18 including to at least the following servers: (i) musemuse.cn; (ii) zhiliaoapp.com; (iii)
19 mob.com; and (iv) umeng.com.

20 73. The private and personally-identifiable TikTok user data and content
21 transferred to one or more of these four China-based servers includes biometrics and
22 User/Device Identifiers. Additional private and personally-identifiable TikTok user data
23 and content transferred to one or more of these four China-based servers includes: (i) a list
24 of the other apps installed on users' mobile devices; and (ii) more specific location data.
25 Such information reveals TikTok users' precise physical location, including possibly
26 indoor locations within buildings, and TikTok users' apps that possibly reveal mental or
27 physical health, religious views, political views, and sexual orientation.

1 **2. Defendants’ Privacy Policies Do Not Constitute Notice Of Or**
 2 **Consent To The Transfer Of Private And Personally-Identifiable**
 3 **TikTok User Data And Content To Servers In China.**

4 74. TikTok users do not knowingly consent to Defendants’ privacy policies
 5 because notice and warnings of the privacy policies are not adequately displayed, as
 6 discussed above. Additionally, many provisions of the privacy policies are ambiguous,
 7 providing inadequate notice of what private and personally-identifiable user data and
 8 content is taken and where it is being sent. Notably, even scholars with expertise in such
 9 matters, such as Mr. Carroll, cannot discern what is being taken and where it is going.
 10 Certainly, ordinary TikTok users cannot be expected to understand such baffling
 11 “disclosures.” This ambiguity further renders the notice inadequate to establish informed
 12 user consent.

13 75. In addition to the above-stated deficiencies, privacy policy provisions stating
 14 that certain TikTok user data and content will be sent to servers in China is contradicted by
 15 Defendants’ public assurances that no such transfers occur. Moreover, TikTok users whose
 16 data and content is sent before they even have an opportunity to sign-up and create an
 17 account do not actually or constructively receive notice, and therefore cannot be deemed to
 18 have assented to, such transfers to China.

19 **3. The China-Based Tech Giants Also Possess TikTok Users’ Private**
 20 **And Personally-Identifiable Data And Content While They Work**
 21 **Cooperatively With The Chinese Government.**

22 76. The bugly.qq.com server is owned and operated by China-based tech giant
 23 Tencent Holdings Limited (“Tencent”), and the umeng.com server is owned and operated
 24 by another China-based tech giant Alibaba Holding Group Limited (“Alibaba”). Tencent
 25 and Alibaba thus possess TikTok users’ private and personally-identifiable data and
 26 content. Such data transfers to Tencent and Alibaba servers were accomplished through
 27 Tencent and Alibaba source code that Defendants embedded within the TikTok app.

28 77. Also embedded within the TikTok app is source code from China-based tech

1 giant Baidu, Inc. (“Baidu”) as well as source code from a China-based software
 2 development kit (“SDK”) known as Igexin. The Igexin SDK is notorious for causing the
 3 removal of some 500 apps from the Google play store in 2017 after it was discovered that
 4 Igexin constituted a “secret backdoor” that allowed its operators “to install a range of
 5 spyware.”⁵⁹ Specifically, Igexin “could update the app to include spyware at any time, with
 6 no warning. The most serious spyware installed on phones were packages that stole call
 7 histories, including the time a call was made, the number that placed the call, and whether
 8 the call went through. Other stolen data included GPS locations, lists of nearby Wi-Fi
 9 networks, and lists of installed apps.”⁶⁰

10 78. Baidu, Alibaba, and Tencent – popularly known by the acronym “BAT” –
 11 are “China’s original tech titans”⁶¹ and dominate the fields of artificial intelligence, social
 12 media, and the internet in China. The private and personally-identifiable TikTok user data
 13 and content they possess may well be used by the Chinese government in the future, if it
 14 has not already.

15 79. BAT routinely assist the Chinese government in the surveillance and control
 16 of its people through biometrics. “Biometric surveillance powered by artificial intelligence
 17 is categorically different than any surveillance we have seen before. It enables real-time
 18 location tracking and behavior policing of an entire population at a previously impossible
 19 scale.”⁶² The Chinese government is taking full advantage of China-based technology
 20 corporations like BAT to assist: “Beijing is embracing technologies like facial recognition
 21 and artificial intelligence to identify and track 1.4 billion people. It wants to assemble a
 22 vast and unprecedented national surveillance system, with crucial help from its thriving

23
 24 ⁵⁹ <https://arstechnica.com/information-technology/2017/08/500-google-play-apps-with-100-million-downloads-had-spyware-backdoor/>.

25 ⁶⁰ <https://arstechnica.com/information-technology/2017/08/500-google-play-apps-with-100-million-downloads-had-spyware-backdoor/>.

26 ⁶¹ <https://www.forbes.com/sites/rebeccafannin/2019/08/23/baidu-alibaba-tencent-clash-to-lead-chinas-tech-future-while-a-new-b-arises/#18cc42e414d0>.

27 ⁶² <https://www.buzzfeednews.com/article/evangreer/dont-regulate-facial-recognition-ban-it>.

1 technology industry. ... China has become the world's biggest market for security and
 2 surveillance technology, with analysts estimating the country will have almost 300 million
 3 cameras installed by 2020. Chinese buyers will snap up more than three-quarters of all
 4 servers designed to scan video footage for faces⁶³

5 80. The Chinese government relies on China-based technology companies like
 6 BAT to assist in government investigations of criminal activity and political dissent, as
 7 well as surveillance activities: "The Chinese police 'request data from Alibaba for their
 8 own investigations, ... tapping into the trove of information the tech giant collects through
 9 its e-commerce and financial payment networks. ... Companies including Alibaba [],
 10 Tencent [], and Baidu [] are required to help China's government hunt down criminal
 11 suspects and silence political dissent. Their technology is also being used to create cities
 12 wired for surveillance. ... Apple disclosed that more than 35,000 user accounts were
 13 affected by 24 Chinese law-enforcement requests in the first half of this year [2017], many
 14 in connection with fraud investigations. It said it provided information on about 90% of
 15 them. Chinese companies don't release any information on the number of requests from
 16 the government, the nature of the requests or the compliance rate.'⁶⁴

17 81. The Chinese government's use of BAT to sort and analyze information,
 18 including information gathered from smartphones, is also well documented: "Along with
 19 access to online data, China's government wants something else from tech companies – the
 20 cloud computing prowess to sort and analyze information. China wants to crunch data
 21 from surveillance cameras, smartphones, government databases and other sources to create
 22 so-called smart cities and safe cities. ... Police now work with Alibaba to use surveillance
 23 footage and data processing to identify 'persons of interest' and keep them out, local police
 24 official Dai Jinming said at a recent conference sponsored by Alibaba. Tencent is working
 25 with police in the southern city of Guangzhou to build a cloud-based 'early-warning

26 ⁶³ <https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html>.

27 ⁶⁴ <https://www.wsj.com/articles/chinas-tech-giants-have-a-second-job-helping-the-government-see-everything-1512056284>.
 28

1 system' that can track and forecast the size and movement of crowds, according to a
2 statement from the Guangzhou police bureau."⁶⁵

3 82. The *Wall Street Journal* has reported on the significant patronage that BAT
4 receive from the Chinese government, the growing number of tech entrepreneurs who have
5 become members of the legislature under President Xi Jinping (including, for example,
6 Tencent's Tony Ma), and BAT's pledges of loyalty to the Chinese government.⁶⁶ "The
7 government is always the boss and the tech firms are there to serve the goals of the
8 Chinese government."⁶⁷

9 83. Defendant Beijing ByteDance is emerging as a threat to BAT's exclusive
10 status: "there's a new B in the BAT trio on the horizon: the world's highest-valued
11 unicorn, ByteDance"⁶⁸ Like BAT, Defendant Beijing ByteDance is subject to the same
12 cybersecurity laws mandating cooperation with the Chinese government that are described
13 in Senator Schumer and Senator Cotton's letter. Senator Hawley, according to the *Wall*
14 *Street Journal*, described the resulting threat to TikTok users by stating: "all it takes is one
15 knock on the door of their parent company [Defendant Beijing ByteDance], based in
16 China, from a Communist Party official for that data [from Defendant TikTok, Inc.] to be
17 transferred to the Chinese government's hands, whenever they need it."⁶⁹ In the same *Wall*
18 *Street Journal* article, a former TikTok employee from the Los Angeles office stated that:
19 "We're a Chinese company ... We answer to China."⁷⁰

20 _____
21 ⁶⁵ <https://www.wsj.com/articles/chinas-tech-giants-have-a-second-job-helping-the-government-see-everything-1512056284>.

22 ⁶⁶ <https://www.wsj.com/articles/the-godfathers-of-chinese-tech-get-an-offer-they-cant-refuse-1520510404>.

23 ⁶⁷ <https://www.wsj.com/articles/the-godfathers-of-chinese-tech-get-an-offer-they-cant-refuse-1520510404>.

24 ⁶⁸ <https://www.forbes.com/sites/rebeccafannin/2019/08/23/baidu-alibaba-tencent-clash-to-lead-chinas-tech-future-while-a-new-b-arises/#18cc42e414d0>.

25 ⁶⁹ <https://www.wsj.com/articles/tiktok-looking-at-ways-to-shake-off-its-ties-to-china-11574073001>.

26 ⁷⁰ <https://www.wsj.com/articles/tiktok-looking-at-ways-to-shake-off-its-ties-to-china-11574073001>.

1 84. A *Washington Post* opinion piece entitled “Could TikTok allow China to
 2 export repression?” describes the danger to TikTok users in the United States if
 3 Defendants provide such users’ private and personally-identifiable data and content to the
 4 Chinese government: “TikTok’s leaders protest that they store local information locally, so
 5 whatever data the company has on the behavioral patterns or personal attributes of some of
 6 the most vulnerable American citizens are not ‘subject to Chinese law.’ But it’s reasonable
 7 to wonder whether TikTok might not comply with targeted intelligence requests from the
 8 repressive regime ruling over its parent company ByteDance. TikTok’s younger users will
 9 be voting in the coming years; down the line, they may hold positions of power. A trove of
 10 their information is a valuable asset.”⁷¹

11 85. The *Wall Street Journal*, in an article entitled “U.S. Orders Chinese Firm to
 12 Sell Dating App Grindr Over Blackmail Risk,” also has reported on the dangers Americans
 13 face from the Chinese government’s accumulation of their private and personally-
 14 identifiable data and content, including blackmail and other sinister scenarios: “U.S.
 15 national-security experts said Chinese government knowledge of an individual’s usage of
 16 Grindr could be used in certain cases to blackmail U.S. officials and others with security
 17 clearances, such as defense contractors, and force them to provide information or other
 18 support to China. They have also envisioned more elaborate scenarios. For example, one
 19 could use Grindr’s location data to discern that a certain user works at a
 20 telecommunications firm and pays regular visits to the same building in Northern Virginia
 21 that intelligence officials frequent. Chinese-intelligence officials could then determine that
 22 that individual is the telecommunications firm’s intelligence liaison, and they would know
 23 both whom to target and how to threaten that person with potentially compromising
 24 information. ... The risk has grown as the Chinese government acquires more large data
 25 sets through hacking and other means, allowing it to build databases with detailed profiles

26 _____
 27 [11574073001.](https://www.washingtonpost.com/opinions/global-opinions/could-tiktok-allow-china-to-export-repression/2019/11/02/1729f038-fa79-11e9-8906-ab6b60de9124_story.html)

28 ⁷¹ https://www.washingtonpost.com/opinions/global-opinions/could-tiktok-allow-china-to-export-repression/2019/11/02/1729f038-fa79-11e9-8906-ab6b60de9124_story.html.

1 of targets.”⁷²

2 **VI. DEFENDANTS’ THEFT OF TIKTOK USER BIOMETRICS.**

3 **A. The Illinois Biometric Information Privacy Act Regulates Face**
 4 **Geometry Scans, Voiceprints And Information Derived Therefrom.**

5 86. In 2008, Illinois enacted the Biometric Information Privacy Act (“BIPA”),
 6 740 ILCS 14/1, *et seq.* This was due to the “very serious need [for] protections for the
 7 citizens of Illinois when it [comes to their] biometric information.” Illinois House
 8 Transcript, 2008 Reg. Sess. No. 276. The Illinois Legislature recognized the importance of
 9 protecting the privacy of individuals’ biometric data, finding that “[b]iometrics are unlike
 10 other unique identifiers that are used to access finances or other sensitive information.”
 11 740 ILCS 14/5(c). “For example, social security numbers, when compromised, can be
 12 changed. Biometrics, however, are biologically unique to the individual; therefore, once
 13 compromised, the individual has no recourse [and] is at heightened risk for identity theft
 14” *Id.*

15 87. BIPA thus focuses on “biometric identifiers” and “biometric information.”
 16 Biometric identifiers consist of “a retina or iris scan, fingerprint, voiceprint, or scan of
 17 hand or face geometry.” 740 ILCS 14/10. A “scan” under BIPA means to examine by
 18 observation or checking, or systematically in order to obtain data especially for display or
 19 storage. *In re Facebook Biometric Information Privacy Litigation*, 2018 WL 2197546, *3
 20 (N.D. Cal. May 14, 2018). “Geometry” under BIPA is the relative arrangement of parts or
 21 elements. *Id.* Neither the term “scan” nor the term “geometry” require “actual or express
 22 measurements of spatial quantities like distance, depth, or angles.” *Id.* Biometric
 23 information constitutes “any information, regardless of how it is captured, converted,
 24 stored, or shared, based on an individual’s biometric identifier used to identify an
 25 individual.” 740 ILCS 14/10.

26

27

28 ⁷² <https://www.wsj.com/articles/u-s-orders-chinese-company-to-sell-grindr-app-11553717942>.

1 **B. Defendants Unlawfully Collect, Use And Profit From TikTok User**
 2 **Biometrics, Face Geometry Scans, Voiceprints And Information Derived**
 3 **Therefrom.**

4 88. Defendants' unlawful collection, possession, storage, dissemination, use and
 5 profiting from biometrics, face geometry scans and voiceprints of TikTok users, and the
 6 information derived therefrom, takes three forms.

7 89. *First*, Defendants' BIPA and other biometrics-related violations are
 8 established by the functionality and code of the TikTok app itself. This functionality and
 9 code includes: (a) content recommendations based on TikTok users' race/ethnicity and
 10 age; (b) scans of face geometry to determine TikTok users' age; (c) censoring video
 11 content to remove people Defendants consider "ugly"; (d) the augmented reality feature
 12 that scans face geometry while processing users' videos; (e) code for deepfake videos; and
 13 (f) code for age, race/ethnicity and emotion recognition.

14 90. *Second*, Defendants' BIPA and other biometrics-related violations are
 15 further established by their ongoing work in China, which includes: (a) the application of
 16 facial recognition technology⁷³ to TikTok users' videos by highly-trained engineers skilled
 17 in computer vision, convolutional neural network and machine learning; (b) patent
 18 applications for face, voice, age, race/ethnicity and emotion recognition technologies; and
 19 (c) the publicly-known functionality of Douyin that allows its users to perform facial
 20 recognition on faces selected by such users from other users' videos.

21 91. *Third*, Defendants' BIPA and other biometrics-related violations are also
 22 established by Defendants' legal and political obligations to accumulate and share vast
 23 troves of data, including biometrics, in order to assist the Chinese government in meeting
 24 two crucial and intertwined state objectives: (a) world dominance in artificial intelligence;

25 ⁷³ Facial recognition "is a technology capable of identifying or verifying a person from a digital
 26 image or a video frame from a video source. There are multiple methods in which facial
 27 recognition systems work, but in general, they work by comparing selected facial features from a
 28 given image with faces within a database." See
https://en.wikipedia.org/wiki/Facial_recognition_system.

1 and (b) population surveillance and control.

2 **1. Defendants’ BIPA And Other Biometrics-Related Violations Are**
 3 **Evidenced By The TikTok App’s Functionality And Code.**

4 92. There are six specific categories of functions and code within the TikTok app
 5 that reveal BIPA violations: the race/ethnicity and age-based content recommendations;
 6 the scans to determine age; the removal of so-called “ugly” videos; the augmented reality
 7 feature; the deepfake video code; and the age, race/ethnicity and emotion recognition
 8 code.⁷⁴ These also evidence violations of the other statutory, constitutional and common
 9 law claims set forth herein.

10 93. That the TikTok app violates BIPA and other laws is highlighted by
 11 comments from a “Bytedance representative” who confessed to *The Verge* that “TikTok
 12 makes use of the company’s AI technologies in various ways, from *facial recognition for*
 13 *the filters* through to the recommendation engine in the For You feed. ... We build
 14 intelligent machines that are capable of understanding and analyzing text, images and
 15 *videos* using natural language processing and computer vision technology. This enables us
 16 to serve users with the content that they find most interesting”⁷⁵

17 94. Similarly, *Marketing Technology Insights* reported on Defendants’ use of
 18 facial recognition technology in the TikTok app in violation of BIPA and other laws,
 19 stating that Defendant TikTok, Inc. and the TikTok app “deploy[] AI and *Face*
 20 *Recognition technology* to analyze user’s interests and preferences through their
 21 interactions with the content, and display a personalized content feed to each user.”⁷⁶

22 **a. Race/Ethnicity And Age Based Content Recommendations.**

23 95. Marc Faddoul, a researcher at the University of California at Berkeley who

24

 25 ⁷⁴ This evidence also constitutes a basis for the other statutory, constitutional and common law
 causes of action herein.

26 ⁷⁵ <https://www.theverge.com/2018/11/30/18107732/bytedance-valuation-tiktok-china-startup>
 (emphasis added).

27 ⁷⁶ <https://martechseries.com/mts-insights/staff-writers/pay-attention-to-tiktok-content/> (emphasis
 28 added).

1 studies artificial intelligence, conducted an experiment in or about February 2020 that
 2 revealed the TikTok app recommends content based in part on race/ethnicity and age
 3 information that it gleans from TikTok users' digital face images. *Buzzfeed* described his
 4 findings: "In the app, when a person follows a new account, they can click an arrow
 5 that then recommends other accounts to follow. Faddoul noticed that when he did this,
 6 the recommended accounts tended to look just like whoever he'd just followed —
 7 right down to ethnicity and hair color."⁷⁷

8 96. *Recode* also reported on Faddoul's research in its article entitled "There's
 9 Something Strange About TikTok Recommendations":

10 When artificial intelligence researcher Marc Faddoul joined TikTok a few
 11 days ago, he saw something concerning: When he followed a new account,
 12 the profiles recommended by TikTok seemed eerily, physically similar to the
 13 profile picture of the first account. Following a young-looking blond woman,
 14 for instance, yielded recommendations to follow more young-looking blond
 15 women. ...

16 Following black men led to recommendations to follow more black men.
 17 Following white men with beards produced recommendations for more white
 18 men with beards. Following elderly people spawned recommendations for
 19 other elderly people. And on and on. ...

20 Faddoul also told *Recode* that he believes it's more likely that TikTok is
 21 using something he calls automatic featurization. This type of
 22 recommendation algorithm could take "signals" from profile images to find
 23 profile pictures with similar attributes. These kinds of signals would be
 24 correlations between the pictures, which could correspond to anything from
 25 skin color to having a beard. The algorithm is simply looking for similarities
 26 in the photos or profiles. ...

27
 28 ⁷⁷ <https://www.buzzfeednews.com/article/laurenstrapagiel/tiktok-algorithim-racial-bias>.

1 “What I suspect is happening is that TikTok is featurizing the profile
2 picture,” he says, “and using these features in the recommendation engine.”⁷⁸

3 **b. Face Scans To Determine Age.**

4 97. Defendants also scan face images taken from TikTok user videos in order to
5 determine TikTok users’ age. The *Wall Street Journal* has reported that “TikTok has built
6 an artificial intelligence tool that scans faces in videos to estimate users’ ages.”⁷⁹ Both
7 Faddoul’s research and this *Wall Street Journal* article are consistent with evidence of
8 Defendants’ work in China on TikTok user videos as well as their patent applications in
9 China for face, voice, age, race/ethnicity and emotion recognition technologies (below).

10 **c. Removal Of Videos Of So-Called “Ugly” People.**

11 98. Public reporting indicates that “the makers of TikTok ... instructed
12 moderators to suppress posts created by users deemed too ugly Today, *The Intercept*
13 and *The Intercept Brasil* are publishing two internal TikTok moderation documents
14 One ... describes algorithmic punishments for unattractive and impoverished users. The
15 documents appear to have been originally drafted in Chinese and later — at times
16 awkwardly — translated into English for use in TikTok’s global offices.”⁸⁰ Defendant
17 TikTok, Inc. uses artificial intelligence technology in its Culver City office to review and
18 flag user content. Given the presence of this AI technology and the sheer volume of
19 TikTok user videos that are reviewed for “ugliness,” it is apparent that Defendant TikTok,
20 Inc. is using facial recognition technology to identify and remove such users’ videos.

21 **d. Augmented Reality Features.**

22 99. The TikTok app uses an advanced video editor and camera face filters.
23 Employing this technology, TikTok users edit their videos to, among other things, morph
24 their face into another face; change the size, shape, height and width of their face; change

25
26 ⁷⁸ <https://www.vox.com/recode/2020/2/25/21152585/tiktok-recommendations-profile-look-alike>.

27 ⁷⁹ <https://www.wsj.com/articles/tiktok-wants-to-grow-up-but-finds-it-tough-to-keep-kids-out-11581858006>.

28 ⁸⁰ <https://theintercept.com/2020/03/16/tiktok-app-moderators-users-discrimination/>.

1 particular features of their face (*e.g.*, eyes, ears, nose, lips, mouth, cheeks), including the
 2 size and shape of such facial features; and so on. Users thereby create videos in which their
 3 faces and specific facial features take on cartoonish dimensions and appearances, and in
 4 which they can appear older, etc.

5 100. This functionality is a form of augmented reality (“AR”).⁸¹ To perform AR,
 6 the TikTok app examines, detects and localizes the face and the arrangement of its various
 7 parts (*e.g.*, the eyes, ears, nose, lips, mouth, cheeks) relative to the other parts, and then
 8 also tracks the face and its various parts (and their relative arrangement) while in motion.

9 101. The following relevant code is located within the TikTok app:

10 “FaceDetectManager”; “faceDetectMaxTime”; “faceDetectMinTime”;
 11 “Requirement_Face_3D_Detect”; “Requirement_Face_Detect”;
 12 “Requirement_Face_Track”; “face_track.model”; “maxScanTime”; “minScanTime”; and
 13 “faceID”. Additional code for pitch, yaw and roll – “the three dimensions of movement
 14 when an object moves through a medium”⁸² – is within the TikTok app as well.

15 102. This functionality and code reveal Defendants’ use of face geometry scans
 16 on TikTok users. While it is currently unclear whether Defendants upload such face
 17 geometry scans from TikTok users’ mobile devices, in addition to performing separate
 18 face geometry scans at the server level, this functionality and code demonstrate
 19 Defendants’ technological ability and willingness to perform such scans on TikTok users.

22 ⁸¹ AR “is an interactive experience of a real-world environment where the objects that reside in the
 23 real world are enhanced by computer-generated perceptual information AR can be defined as a
 24 system that fulfills three basic features: a combination of real and virtual worlds, real-time
 25 interaction, and accurate 3D registration of virtual and real objects. ... This experience is
 26 seamlessly interwoven with the physical world such that it is perceived as an immersive aspect of
 27 the real environment. In this way, augmented reality alters one’s ongoing perception of a real-
 world environment With the help of advanced AR technologies (*e.g.* adding computer vision,
 incorporating AR cameras into smartphone applications and object recognition) the information
 about the surrounding real world of the user becomes interactive and digitally manipulated.” *See*
https://en.wikipedia.org/wiki/Augmented_reality.

28 ⁸² https://simple.wikipedia.org/wiki/Pitch,_yaw,_and_roll.

1 **e. Code For Deepfake Videos.**

2 103. There is code within the TikTok app, as well as within Douyin, for
 3 performing facial recognition. *TechCrunch* reported that there is “Face Swap” code within
 4 the TikTok app for “life-like deepfakes technology.” It “asks users to take a multi-angle
 5 biometric scan of their face, then choose from a selection of videos they want to add their
 6 face to and share.”⁸³ Defendants admitted that such code is present in the TikTok app, but
 7 denied its use. A TikTok spokesperson “insisted that ‘after checking with the teams I can
 8 confirm this is definitely not a function in TikTok’ They later told *TechCrunch* that
 9 ‘the inactive code fragments are being removed to eliminate any confusion,’ which
 10 implicitly confirms that Face Swap code was found in TikTok.”⁸⁴

11 104. That the “Face Swap” code is present in the TikTok app demonstrates
 12 Defendants’ technological capacity and intent to perform facial recognition on TikTok
 13 users. Further, the “Face Swap” code further confirms the direct involvement of Defendant
 14 Beijing ByteDance in the TikTok app, because there would otherwise be no way for the
 15 TikTok app to include facial recognition code that Defendants TikTok, Inc. and
 16 ByteDance, Inc. have denied was ever used in the United States.

17 **f. Code For Age, Race/Ethnicity And Emotion Recognition.**

18 105. There is additional code within the TikTok app designed to recognize users’
 19 age, race/ethnicity and emotions. The code separates race/ethnicity into at least four
 20 categories: “Blac” [*sic.*]; “Indian”; “White”; and “Yellow.” The code also distinguishes
 21 between at least seven different ranges of emotion: “Angry”; “Disgust”; “Fear”; “Happy”;
 22 “Neutral”; “Sad”; and “Surprise.”

23 106. To place TikTok users within one of these categories, the TikTok app would
 24 have to use face geometry scans and/or voiceprints. It is currently unclear whether this
 25 code is active at the mobile device level and, if so, whether Defendants upload any such
 26 _____

27 ⁸³ <https://techcrunch.com/2020/01/03/tiktok-deepfakes-face-swap/>.

28 ⁸⁴ <https://techcrunch.com/2020/01/03/tiktok-deepfakes-face-swap/>.

1 face geometry scans and voiceprints from TikTok users' mobile devices. Nonetheless, the
 2 age, race/ethnicity and emotion recognition code within the TikTok app is consistent with
 3 Faddoul's research (above) and also directly correlates to Defendants' China-based work
 4 on TikTok user videos and patent applications (below).

5 **2. Defendants' BIPA And Other Biometrics-Related Violations Are**
 6 **Further Evidenced By Defendants' China-Based Operations.**

7 107. Defendants' BIPA violations are further established by their ongoing work in
 8 China, which includes: (a) the application of facial recognition technology to TikTok
 9 users' videos by highly-trained engineers skilled in computer vision, convolutional neural
 10 network and machine learning; (b) patent applications for face, voice, age, race/ethnicity
 11 and emotion recognition technologies; and (c) the Douyin app's functionality that allows
 12 its users to perform facial recognition on faces selected by such users from other users'
 13 videos. These factors also evidence violations of the other statutory, constitutional and
 14 common law claims set forth herein.

15 **a. Defendants' China-Based Team Of Highly-Skilled**
 16 **Computer Vision, Convolutional Neural Network, And**
 17 **Machine Learning Engineers.**

18 108. Defendants' artificial intelligence work within China, which is closely tied to
 19 its United States operations, is among the most sophisticated in the world. "ByteDance has
 20 received accolades for being a top AI innovator from CBInsight who recognized the
 21 company on its 2018 AI 100 List as well as from Fast Company, who placed it on its most
 22 innovative companies list. In 2016, it founded its AI Lab, a research division led by Wei-
 23 Ying Ma, formerly of Microsoft Research Asia. The Lab's primary focus has been on
 24 developing innovative technologies to enhance ByteDance's content platforms."⁸⁵

25 109. Defendants have a team of engineers in cutting-edge fields such as computer
 26

27 ⁸⁵ [https://www.forbes.com/sites/bernardmarr/2018/12/05/ai-in-china-how-buzzfeed-rival-](https://www.forbes.com/sites/bernardmarr/2018/12/05/ai-in-china-how-buzzfeed-rival-bytedance-uses-machine-learning-to-revolutionize-the-news/#6579bada40db)
 28 [bytedance-uses-machine-learning-to-revolutionize-the-news/#6579bada40db.](https://www.forbes.com/sites/bernardmarr/2018/12/05/ai-in-china-how-buzzfeed-rival-bytedance-uses-machine-learning-to-revolutionize-the-news/#6579bada40db)

1 vision,⁸⁶ convolutional neural network (“CNN”),⁸⁷ and machine learning,⁸⁸ all of which are
 2 foundational to the face geometry scans and voiceprints that Defendants conduct on and/or
 3 derive from the Private Videos and the posted videos of TikTok users.

4 110. Defendants’ China-based engineering team includes, among others: (i) a
 5 research scientist focused on facial recognition, object detection, computer vision and
 6 machine learning who has worked for Defendants since 2018; (ii) a computer vision and
 7 image processing algorithm engineer who has worked for Defendants since 2017; (iii) a
 8 computer vision algorithm engineer who has worked for Defendants since 2019; (iv) a
 9 machine learning and neural network engineer who has worked for Defendants since 2017;
 10 (v) an algorithm engineer who focuses on video retrieval and who has worked for
 11 Defendants since 2018; and (vi) an algorithm engineer who has worked for Defendants

12 ⁸⁶ Computer vision “is an interdisciplinary scientific field that deals with how computers can gain
 13 high-level understanding from digital images or videos. ... Computer vision tasks include methods
 14 for acquiring, processing, analyzing and understanding digital images The classical problem in
 15 computer vision, image processing, and machine vision is that of determining whether or not the
 16 image data contains some specific object, feature, or activity. ... • Object recognition (also called
 17 object classification) – one or several pre-specified or learned objects or object classes can be
 18 recognized, usually together with their 2D positions in the image or 3D poses in the scene. ... •
 19 Identification – an individual instance of an object is recognized. Examples include identification
 20 of a specific person’s face or fingerprint • Detection – the image data are scanned for a specific
 21 condition. ... Currently, the best algorithms for such tasks are based on convolutional neural
 22 networks. ... Several specialized tasks based on recognition exist, such as: • Content-based image
 23 retrieval – finding all images in a larger set of images which have a specific content. ... • Facial
 24 recognition.” See https://en.wikipedia.org/wiki/Computer_vision#Recognition.

25 ⁸⁷ CNN “is a class of deep neural networks, most commonly applied to analyzing visual imagery.
 26 ... They have applications in image and video recognition, recommender systems, [and] image
 27 classification CNNs use relatively little pre-processing compared to other image classification
 28 algorithms. This means that the network learns the filters that in traditional algorithms were hand-
 engineered. This independence from prior knowledge and human effort in feature design is a
 major advantage.” See https://en.wikipedia.org/wiki/Convolutional_neural_network#Image_recognition.

⁸⁸ Machine learning “is the study of computer algorithms that improve automatically through
 experience. It is seen as a subset of artificial intelligence. Machine learning algorithms build a
 mathematical model based on sample data, known as “training data”, in order to make predictions
 or decisions without being explicitly programmed to do so. Machine learning algorithms are used
 in a wide variety of applications, such as ... computer vision, where it is difficult or infeasible to
 develop conventional algorithms to perform the needed tasks.” See https://en.wikipedia.org/wiki/Machine_learning.

1 since 2017.

2 **b. Facial Recognition Technology Applied To TikTok Videos.**

3 111. Wei-Ying Ma is a ByteDance Vice President in Beijing and has led the AI
4 Lab since 2017. He is known for having developed a highly respected image retrieval
5 system called NeTra, which is a tool for navigating very large image databases. Ma
6 recently delivered a keynote speech at a Taipei Web Conference in which he
7 acknowledged that Defendants use facial recognition technology and face geometry scans
8 on their enormous and ever-growing database of face images from user videos. During his
9 speech, Ma used visual representations that show facial recognition and face geometry
10 scans being performed on specific regions of face images. Chinese language text
11 accompanying the face images indicate the type of facial expression and the age of the
12 individuals represented by the face images. English language notes to the side of the face
13 images refer to “emotion analysis,” “object detection and tracking,” and “content-based
14 recommendation.” Ma made the following representations during his speech while these
15 face images, accompanied by the aforementioned Chinese language and English language
16 statements, were visually presented on the screen:

17 We are actually receiving a huge number of video created by users every
18 day, so it’s at the hundreds of millions of video per day. Imagine the amount
19 of computation and also video understanding we need to do here. And here
20 just to give you a glimpse of all kinds of video understanding tasks we need
21 to run, and let me show you for example, you just saw that video, and for
22 video like that we actually do all kind of analysis. We need to automatically
23 classify and also do a lot tagging and understand the structure inside the
24 video and also run copyright infringement detecting and duplicate detection
25 and also object detection and tracking. So based on this video, we convert
26 this video into a structural representation, and here just to give you one of the
27
28

1 examples.⁸⁹

2 112. Defendants’ team of engineers in China also includes a computer vision and
3 machine learning engineer who has worked for Defendants since 2018. His job
4 responsibilities have included face/body detection and face attribute recognition, *including*
5 *specifically on TikTok users’ videos*.

6 113. Within China, Defendant Beijing ByteDance makes no secret of its
7 processing and analysis of users’ videos from around the world. *TechNode* reported that
8 one of its vice presidents publicly told a gathering that “ByteDance” required more chips
9 to continue uploading, processing and analyzing its vast database of videos accumulated
10 from around the world. This vice president stated that “‘Bytedance has the largest number
11 of users in *the world* whose *videos* need to be analyzed and processed and uploaded, and
12 we are purchasing a large number of chips.’”⁹⁰

13 114. Defendants’ wealth of video recordings from TikTok users is critical to
14 Defendants’ success in making the TikTok app one of the most popular in the world: “The
15 [TikTok] app heavily utilizes AI that is trained on the vast quantity of *video footage* to
16 understand the preferences of users, while also using machine learning to make creating,
17 editing, and promoting the *videos* as easy as possible.”⁹¹

18 115. Indeed, “*all of ByteDance’s products* use artificial intelligence and machine
19 learning to deliver content that users want. The company’s intelligent machines use
20 computer vision and natural language processing technology to understand and analyze
21 written content, images and *videos*. Then, based upon what the machines know about each
22 user, they deliver the content it believes each user would want. As a user interacts with the
23 content by taps, swipes, time spent with each article, comments and more, large-scale
24 machine learning and deep learning algorithms continue to learn about a user’s preferences

25
26 ⁸⁹ <https://www.youtube.com/watch?v=2D29f4-J2mw> (at 18:18 – 19:17).

27 ⁹⁰ <https://technode.com/2018/04/24/bytedance-jinri-toutiao-ai-chips/> (emphasis added).

28 ⁹¹ <https://dzone.com/articles/the-data-thats-driving-chinas-hidden-champions> (emphasis added).

1 to refine its content delivery for the future. The end result is a high-quality content feed
 2 based upon each user's preferences and interests. As more content is accumulated by the
 3 system, the better the algorithms get to enhance the content experience."⁹²

4 **c. Face, Age, Race/Ethnicity And Emotion Recognition Patent**
 5 **Applications.**

6 116. One of Defendants' engineers in China stands out for his inventions that
 7 form the basis of numerous patent applications filed by Defendants' sister company
 8 Beijing ByteDance Network Technology Co., Ltd. The underlying technology in these
 9 patent applications involves age, race and emotion detection through face images,
 10 including those derived from videos. The specific patent applications include, among
 11 others, the following:

- 12 a. Facial image identifying method.⁹³
- 13 b. Use of face images and a facial recognition model to determine ethnic
 14 information, to then determine race, to ultimately determine age.⁹⁴
- 15 c. Use of face and body images, and a facial recognition model, to
 16 determine age.⁹⁵
- 17 d. Use of image data sets and audio data sets to determine age.⁹⁶
- 18 e. Use of face images extracted from videos to determine age.⁹⁷
- 19 f. Use of face images extracted from videos to determine age.⁹⁸
- 20 g. Human facial expression recognition method.⁹⁹

22 ⁹² [https://www.forbes.com/sites/bernardmarr/2018/12/05/ai-in-china-how-buzzfeed-rival-](https://www.forbes.com/sites/bernardmarr/2018/12/05/ai-in-china-how-buzzfeed-rival-bytedance-uses-machine-learning-to-revolutionize-the-news/#6579bada40db)
 23 [bytedance-uses-machine-learning-to-revolutionize-the-news/#6579bada40db](https://www.forbes.com/sites/bernardmarr/2018/12/05/ai-in-china-how-buzzfeed-rival-bytedance-uses-machine-learning-to-revolutionize-the-news/#6579bada40db) (emphasis added).

24 ⁹³ Publication No. WO2020037963A1.

25 ⁹⁴ Publication No. CN110046571A.

26 ⁹⁵ Publication No. CN109993150A.

27 ⁹⁶ Publication No. CN110321863A.

28 ⁹⁷ Publication No. CN110163170A.

⁹⁸ Publication No. CN110188660A.

1 h. Use of face images extracted from videos to determine emotions
2 based on expression recognition.¹⁰⁰

3 i. Use of face images extracted from video segments to identify a face
4 characteristic by parsing the face image.¹⁰¹

5 117. This same engineer was one of the inventors involved in two earlier patent
6 applications filed by a Chinese university that concern face attribute recognition¹⁰² and a
7 face verification method that determines whether faces in two images are the same or
8 distinct.¹⁰³

9 118. “TikTok’s owner, Beijing-based ByteDance, is a hit app factory that has
10 spent the last decade learning how to use artificial intelligence, machine learning, and
11 *facial recognition* to figure out what people like and serve them endless streams of
12 entertainment tailored to their interests and *emotions*. Its apps are used by billions of
13 people, including 1.45 billion global downloads for TikTok alone. The company has years
14 of data informing it on *how people think, feel and act*, making it an expert on *what makes*
15 *people tick and how to persuade them* to watch, share or like certain content.”¹⁰⁴

16 **d. Voiceprint Patent Applications.**

17 119. Beijing ByteDance Network Technology Co., Ltd. filed additional patent
18 applications for a method for voice extraction involving voiceprints,¹⁰⁵ a voice recognition
19 method,¹⁰⁶ and an age recognition method based on audio.¹⁰⁷ This is consistent with
20

21

⁹⁹ Publication No. CN110097004A.

22 ¹⁰⁰ Publication No. CN110175565A.

23 ¹⁰¹ Publication No. CN110163171A.

24 ¹⁰² Publication No. CN106203395B.

25 ¹⁰³ Publication No. CN106203533B.

26 ¹⁰⁴ <https://www.bloomberg.com/news/newsletters/2019-10-29/worries-that-tiktok-is-a-threat-to-national-security-have-merit> (emphasis added).

27 ¹⁰⁵ Publication No. CN110503961A.

28 ¹⁰⁶ Publication No. WO2019214628A1.

1 reporting that Defendant Beijing ByteDance “uses various AI technologies in its services
2 [including] *voice recognition*”¹⁰⁸ In fact, during Wei-Ying Ma’s recent keynote speech
3 at a Taipei Web Conference (above), he discussed the use of audio to identify speakers and
4 he published a slide during his speech entitled “Speaker Identification” that stated: “Detect
5 identity, age, gender of speakers.”¹⁰⁹

6 **e. The Douyin App’s Facial Recognition Function.**

7 120. The Douyin app provides its users with an “in-video” search tool that uses
8 facial recognition technology. Users of Douyin can press the “Search” button while a video
9 is playing, drag a rectangle around the target face in the video, and cause the Douyin app
10 to perform a search (based on the face in question) for other videos in which the targeted
11 person appears.¹¹⁰ This subjects anyone using the Douyin app to “behind-the-scenes *facial*
12 *recognition* analysis.”¹¹¹ While U.S. TikTok users cannot access this feature, there is
13 evidence that they are subject to the same behind-the-scenes facial recognition analysis, as
14 discussed herein.

15 **3. Defendants’ BIPA And Other Biometrics-Related Violations Are**
16 **Also Evidenced By Their Obligation To Accumulate And Share**
17 **Data, Including Biometrics, With The Chinese Government.**

18 121. Defendants’ BIPA violations are further established by Defendants’ legal
19 and political obligations to accumulate and share data, including biometrics, in order to
20 assist the Chinese government in meeting two crucial and intertwined state objectives: (a)
21 world dominance in artificial intelligence; and (b) population surveillance and control.¹¹²

22
23 ¹⁰⁷ Publication No. CN110335626A.

24 ¹⁰⁸ <https://medium.com/syncedreview/intel-and-bytedance-partner-on-ai-lab-b678036cbda4>
25 (emphasis added).

26 ¹⁰⁹ <https://www.youtube.com/watch?v=2D29f4-J2mw> (at 30:04).

27 ¹¹⁰ <https://radiichina.com/tiktok-new-video-search-function-is-from-the-future/>.

28 ¹¹¹ <https://futurism.com/the-byte/tiktok-facial-recognition> (emphasis added).

¹¹² This evidence also constitutes a basis for the other statutory, constitutional and common law

1 **a. The Chinese Government’s Plan To Become The World**
 2 **Leader In Artificial Intelligence.**

3 122. In 2017, the Chinese government released its Next Generation Artificial
 4 Intelligence Development Plan, in which it set 2030 as the temporal goal for becoming the
 5 world leader in artificial intelligence. To ensure achievement of its artificial intelligence
 6 goal, the Chinese government selected the five leading technology companies as “national
 7 champions” and assigned them particular areas of research and development within the
 8 artificial intelligence field. In exchange, these companies receive government support,
 9 including access to finance, preferential contract bidding and sometimes market share
 10 protection. The list of “national champions” has grown to at least 15 in recent years.¹¹³

11 123. The United States government has taken notice. Last November, Congress’s
 12 National Security Commission on Artificial Intelligence, chaired by former Google CEO
 13 Eric Schmidt, published an interim report warning that China was outpacing the United
 14 States in artificial intelligence spending.¹¹⁴

15 **b. The Chinese Government’s Program Of Population**
 16 **Surveillance And Control.**

17 124. The Chinese government’s monitoring of and control over its own
 18 population are well known. Most notable is its pervasive use of artificial intelligence-
 19 enabled cameras to conduct video surveillance of its population.¹¹⁵ As the *South China*
 20 *Morning Post* reported: “China’s goal of becoming a global leader in artificial intelligence
 21 (AI) is nowhere more manifested than in how facial recognition technology has become a
 22 part of daily life in the world’s second-largest economy. Facial recognition systems, which
 23 are biometric computer applications that automatically identify an individual from a
 24 database of digital images, are now being used extensively in areas such as public security,

25 _____
 causes of action herein.

26 ¹¹³ <https://fortune.com/longform/tiktok-app-artificial-intelligence-addictive-bytedance-china/>.

27 ¹¹⁴ <https://fortune.com/longform/tiktok-app-artificial-intelligence-addictive-bytedance-china/>.

28 ¹¹⁵ <https://fortune.com/longform/tiktok-app-artificial-intelligence-addictive-bytedance-china/>.

1 financial services, transport and retail across the country.”¹¹⁶ In fact, the Chinese
 2 government employs a variety of biometrics for population surveillance and control: “In
 3 addition to voice recognition, there are facial and pupil recognition, gathering of DNA
 4 samples—building the world’s largest DNA database—and fingerprint scans.”¹¹⁷

5 c. **Data Accumulation, Including Biometrics, Through China-**
 6 **Based Technology Companies Is A Critical Part Of**
 7 **Achieving The Chinese Government’s Twin Goals.**

8 125. Artificial intelligence algorithms feed on data to learn and improve – thus,
 9 the more data the better the development of the algorithms driving the advance of the
 10 artificial intelligence.¹¹⁸ With better artificial intelligence comes more effective population
 11 surveillance and control.

12 126. To advance these interrelated goals, the Chinese government has worked
 13 hand in glove with China-based technology companies to accumulate and share data. For
 14 example, the China-based company Megvii, a leader in computer vision, has the world’s
 15 largest open source database (Face++) for training other facial recognition algorithms. It
 16 has reportedly used government data banks to help compile this training program.¹¹⁹ As
 17 another example, the Chinese government partnered with the China-based technology firm
 18 d-Ear Technologies to build a database of voiceprints for voice recognition purposes.¹²⁰

19 127. “Private [China-based] corporations and the [Chinese] Communist Party’s
 20 security apparatus have grown together, discovering how the same data sets can both cater
 21 to consumers and help commissars calibrate repression. ... Many [China-based] tech firms

22 _____
 23 ¹¹⁶ <https://www.scmp.com/tech/start-ups/article/2133234/meet-five-chinese-start-ups-pushing-facial-recognition-technology>.

24 ¹¹⁷ <https://vlifestyle.org/codec-news/?l=business/content-2254742-china-gathers-people-s-voices-new-identification-technology-drawing-concerns>.

25 ¹¹⁸ <https://fortune.com/longform/tiktok-app-artificial-intelligence-addictive-bytedance-china/>.

26 ¹¹⁹ <https://fortune.com/longform/tiktok-app-artificial-intelligence-addictive-bytedance-china/>.

27 ¹²⁰ <https://vlifestyle.org/codec-news/?l=business/content-2254742-china-gathers-people-s-voices-new-identification-technology-drawing-concerns>.

1 make a point of hiring the relatives of high party officials, and a vast state database of
 2 headshots might be shared with a private firm to train new facial recognition software,
 3 while the firm's trove of real-time user data might be offered to police, for a panoramic
 4 view of potential 'troublemakers.'"¹²¹

5 128. Such data accumulation is not confined to China's borders. For example, the
 6 Chinese government is compiling a tremendous storehouse of private and personally-
 7 identifiable data on ordinary Americans. Recently, Chinese government-sponsored hackers
 8 stole data belonging to approximately 500 million Marriott International guests.
 9 "[M]achine learning is yielding uses for large data sets that humans alone could not
 10 imagine – or even understand – given that machine learning can generate correlations
 11 among data that the machine itself can't explain.... Beijing's plan may be simply to
 12 vacuum up as much data like this as possible and *then* see what today's machine
 13 learning—or, better yet, tomorrow's machine learning—can do with it."¹²²

14 129. The lengths to which the Chinese government will go to obtain such data
 15 about ordinary Americans is further evidenced by other large-scale hacking schemes,
 16 including one involving 145 million Americans whose data was held by Equifax,¹²³ and
 17 another involving 78 million Americans whose data was held by Anthem.¹²⁴ "The United
 18 States assessed that China was building a vast database of who worked with whom in
 19 national security jobs, where they traveled and what their health histories were, according
 20 to American officials. Over time, China can use the data sets to improve its artificial
 21 intelligence capabilities to the point where it can predict which Americans will be primed
 22 for future grooming and recruitment"¹²⁵ "The hacks, security researchers said, were an

24 ¹²¹ <https://www.nytimes.com/interactive/2019/05/02/opinion/will-china-export-its-illiberal-innovation.html>.

25 ¹²² <https://www.justsecurity.org/62187/weapons-mass-consumerism-china-personal-information/>.

26 ¹²³ <https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html>.

27 ¹²⁴ <https://www.nytimes.com/2019/05/09/technology/anthem-hack-indicted-breach.html>.

28 ¹²⁵ <https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html>.

1 extension of China's evolving algorithmic surveillance system, which has greatly
2 expanded over the past few years."¹²⁶

3 130. The Chinese government's goal of obtaining private and personally-
4 identifiable data (including biometrics) of ordinary citizens throughout the world is also
5 evidenced by the deal struck by China-based CloudWalk Technology in Africa.
6 CloudWalk, with the Chinese government's blessing, entered into a strategic partnership
7 agreement with Zimbabwe to begin a large-scale facial recognition program. With access
8 to a database containing millions of Zimbabwean faces, CloudWalk and the Chinese
9 government intend to train their algorithms in order to further improve their facial
10 recognition capabilities. "With the largest surveillance system already in place, *China is*
11 *also building one of the world's most comprehensive facial recognition databases.*
12 Rolling out the technology in a majority black population will allow CloudWalk to more
13 clearly identify other ethnicities, getting ahead of US and European developers."¹²⁷

14 **d. Defendants Are Obligated By Chinese Law And Politics To**
15 **Accumulate And Secretly Share Their Data, Including**
16 **Biometrics, With The Chinese Government.**

17 131. Given the Chinese government's illegal extraction of massive quantities of
18 private and personally-identifiable data (including biometrics) from hundreds of millions
19 of ordinary Americans and others, there is no reason to believe that the Chinese
20 government has refrained from extracting the same type of U.S. TikTok user data from
21 Defendants. In fact, to access that data, there is no need to hack major U.S. corporations or
22 the China-based technology companies, like Defendants, that have surreptitiously amassed
23 such information on their own. That is because such China-based companies are *required*
24 *by law* to *secretly* provide that data to the government upon demand:

25 The message contained in each of China's state security laws passed since

26 ¹²⁶ <https://www.nytimes.com/2019/05/09/technology/anthem-hack-indicted-breach.html>.

27 ¹²⁷ [https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-](https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/)
28 [dominance-through-diversity/](https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/) (emphasis added).

1 the beginning of 2014 is clear: everyone is responsible for the party-state's
 2 security. According to the CCP's definition of state security, the Party's
 3 political leadership is central. ... And the party expects Chinese people and
 4 citizens to assist in collecting intelligence. The Intelligence Law states 'any
 5 organization and citizen shall, in accordance with the law, support, provide
 6 assistance, and cooperate in national intelligence work, and guard the secrecy
 7 of any national intelligence work that they are aware of...' Not only is
 8 everyone required to participate in intelligence work when asked, but that
 9 participation must be kept secret.¹²⁸

10 132. Consequently, Defendants must "support, provide assistance and cooperate"
 11 by accumulating TikTok user data, including biometrics such as face geometry scans,
 12 voiceprints and information derived therefrom, and then share such data with the Chinese
 13 government. In an article entitled "Take China's TikTok App Security Threat Seriously,"
 14 *Bloomberg* reported that many "Hong Kong protesters say that regardless of whether
 15 TikTok is censoring content or not, they fear posting on a social media site owned by
 16 ByteDance, a Beijing company that must hand over user information to Chinese authorities
 17 if asked, just like all its compatriots."¹²⁹

18 133. In fact, Defendants in this action – including even the two based in the
 19 United States (Defendants TikTok, Inc. and ByteDance, Inc.) – have objected to Plaintiff
 20 Misty Hong's requests for the production of relevant documents in this lawsuit "to the
 21 extent they seek state secrets or any other information that cannot be disclosed without
 22 violating Chinese law, including the People's Republic of China on Guarding State Secrets
 23 and/or Civil Procedure Law of the People's Republic of China ("State Secrets")."
 24 Defendants apparently interposed this "State Secrets" objection in order to comply with

25 _____
 26 ¹²⁸ <https://capx.co/britain-must-avoid-being-sucked-into-huaweis-moral-vacuum/>. See also
 27 <https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense>.

28 ¹²⁹ <https://www.bloomberg.com/news/newsletters/2019-10-29/worries-that-tiktok-is-a-threat-to-national-security-have-merit>.

1 China's Intelligence Law requirement that "[n]ot only is everyone required to participate in
2 intelligence work when asked, but that participation must be kept secret."¹³⁰ This "State
3 Secrets" objection flatly contradicts Defendant TikTok, Inc.'s misleading public statement
4 that "none of our data is subject to Chinese law."¹³¹

5 134. Defendant Beijing ByteDance has a particularly strong incentive to
6 cooperate with the Chinese government. In 2018, China's State Administration of Radio
7 and Television, an arm of the Chinese Communist Party, ordered Defendant Beijing
8 ByteDance to shut down one of its apps due to "vulgar" content. That prompted the CEO
9 of Defendant Beijing ByteDance to publicly apologize. His re-dedication to the Chinese
10 Communist Party resulted in his being named one of the "100 outstanding private
11 entrepreneurs" who were "chosen for being 'emblematic of the country's private economic
12 development', while also being people who 'resolutely uphold the Party's leadership
13'"¹³²

14 135. In a further show of allegiance to the Chinese government, Defendant
15 Beijing ByteDance actively supports and participates in the spreading of Communist Party
16 propaganda. It signed a strategic cooperation agreement with the Ministry of Public
17 Security's Press and Publicity Bureau to promote the credibility of the police department,
18 including within an area of China known for severe repression, demolition of mosques,
19 and wide-spread detention centers for ethnic minorities. Under that agreement, "all levels
20 and divisions of police units from the Ministry of Public Security to county-level traffic
21 police would have their own Douyin account to disseminate propaganda. The agreement
22 also reportedly says ByteDance would increase its offline cooperation with the police
23 department"¹³³

24 _____
25 ¹³⁰ <https://capx.co/britain-must-avoid-being-sucked-into-huaweis-moral-vacuum/>.

26 ¹³¹ <https://newsroom.tiktok.com/en-us/statement-on-tiktoks-content-moderation-and-data-security-practices>.

27 ¹³² <https://chinatechmap.aspi.org.au/#/company/bytedance>.

28 ¹³³ <https://chinatechmap.aspi.org.au/#/company/bytedance>. *See also*

136. Combined with evidence of the TikTok's app's functionality and code, the application of facial recognition technology to TikTok user videos, the patent applications for facial, voice, age, race/ethnicity and emotion recognition technologies, and the Douyin app's facial recognition feature, Defendants' legal obligations and political ties to the Chinese government make clear their large-scale BIPA and other biometrics violations.

VII. DEFENDANTS UNJUSTLY PROFIT WHILE PLAINTIFFS, THE CLASS AND THE TWO SUBCLASSES SUFFER HARM.

137. Defendants use the User/Device Identifiers, the biometric identifiers and information, and the Private Videos and Private Video Images to create a dossier of private and personally-identifiable data and content for each TikTok user. These are living files that are supplemented over time with additional private and personally-identifiable user data and content, and utilized in the past, the present and the future for economic and financial gain.

138. Defendants' unlawful possession and control over these ever-expanding dossiers make tracking and profiling TikTok users, and targeting them with advertising, much more efficient, effective and lucrative. These living dossiers of private and personally-identifiable data and content are used to analyze TikTok users' income, consumption habits, and preferences. Such information provides guidance as to what methods of advertising will be most effective on particular TikTok users, what products – including Defendants' own products – will be most attractive to particular TikTok users, and how much to spend on particular ads. Defendants unjustly have earned and continue to earn substantial profits and revenues from such targeted advertising and from generating increased demand for and use of Defendants' other products.

139. Defendants also unlawfully leverage these living dossiers of private and personally-identifiable TikTok user data and content to improve their artificial intelligence technologies and file patent applications, thereby unjustly increasing their past, present and

https://www.washingtonpost.com/world/tiktoks-owner-is-helping-chinas-campaign-of-repression-in-xinjiang-report-finds/2019/11/28/98e8d9e4-119f-11ea-bf62-eadd5d11f559_story.html.

1 future profits and revenues – and their market value.

2 140. Meanwhile, Plaintiffs, the Class and the Subclasses have incurred, and
3 continue to incur, harm as a result of the invasion of privacy stemming from Defendants'
4 covert theft of their private and personally-identifiable data and content – including their
5 User/Device Identifiers, biometric identifiers and information, and Private Videos and
6 Private Video Images. Plaintiffs, the Class and the Subclasses also have suffered and
7 continue to suffer harm in the form of diminution of the value of their private and
8 personally-identifiable data and content as a result of Defendants' surreptitious and
9 unlawful activities. Moreover, Plaintiffs, the Class and the Subclasses have suffered and
10 continue to suffer injuries to their mobile devices. The battery, memory, CPU and
11 bandwidth of such devices have been compromised, and as a result the functioning of such
12 devices has been impaired and slowed, due to Defendants' clandestine and unlawful
13 activities. Finally, Plaintiffs, the Class and the two Subclasses have incurred additional
14 data usage and electricity costs that they would not have incurred but for Defendants'
15 covert and unlawful actions.

16 **VIII. FRAUDULENT CONCEALMENT AND TOLLING.**

17 141. The applicable statutes of limitations are tolled as a result of Defendants'
18 knowing and active concealment of their unlawful conduct alleged above – through,
19 among other things, their obfuscation of the source code, misleading public statements,
20 and hidden and ambiguous privacy policies and terms of use. Plaintiffs, the Class and the
21 two Subclasses were ignorant of the information essential to pursue their claims, without
22 any fault or lack of diligence on their own part.

23 142. Also, at the time the action was filed, Defendants were under a duty to
24 disclose the true character, quality, and nature of their activities to Plaintiffs, the Class and
25 the two Subclasses. Defendants are therefore estopped from relying on any statute of
26 limitations.

27 143. Defendants' fraudulent concealment is common to the Class and the two
28 Subclasses.

1 **IX. NAMED PLAINTIFF ALLEGATIONS.**

2 **A. The California Plaintiffs.**

3 **1. Plaintiff Misty Hong.**

4 144. Plaintiff Misty Hong is currently a full-time college student. In or about
5 March or April 2019, Ms. Hong downloaded the TikTok app onto her mobile device. At
6 the time Ms. Hong downloaded the TikTok app, she did not read any privacy policy or
7 terms of use, nor did she see discernible hyperlinks to or warnings about these items. In
8 fact, she never clicked the sign-up button and never knowingly created an account with
9 Defendants. However, months later, she discovered for the first time that Defendant
10 TikTok, Inc. had created an account for her, without her knowledge or consent, and
11 provided her with a user name (the word “user” followed by a combination of numbers
12 followed by “@” followed by the word “user” followed by a combination of letters and
13 numbers) and assigned her phone number as the account password.

14 145. Shortly after completing the download of the TikTok app onto her mobile
15 device, Ms. Hong made approximately five or six videos using the TikTok app on her
16 mobile device. Images of her face were captured in some or all of these videos. Ms. Hong
17 experienced difficulty in timing the background music to lip-syncing and dancing.
18 Consequently, after shooting each video, Ms. Hong (i) sometimes pressed the “next”
19 button and (ii) sometimes pressed the “x” button and then the “reshoot” button. Ms. Hong
20 neither saved nor posted any of these videos. But, as a result of sometimes pressing the
21 “next” button, Defendants took some of these Private Videos without Ms. Hong’s
22 knowledge or consent. Images of Ms. Hong’s face also have been captured in Musical.ly
23 and/or TikTok videos recorded and posted by others.

24 146. During the time that the TikTok app was installed on Ms. Hong’s mobile
25 device, Defendants surreptitiously performed the following actions without notice to or the
26 knowledge and consent of Ms. Hong: (i) Defendants took her User/Device Identifiers and
27 Private Videos from her mobile device; (ii) Defendants took her biometric identifiers and
28 information (including face geometry scans and voiceprints) from her and her friends’

1 mobile device and/or videos; (iii) Defendants took her private and personally-identifiable
2 data and content from her mobile device before she had the opportunity to sign up and
3 create an account; (iv) Defendants took her private and personally-identifiable data and
4 content from her mobile device after she closed the TikTok app; and (v) Defendants
5 transferred some or all such stolen data and content to servers located in China – including
6 to servers under the control of third-parties who cooperate with the Chinese government.

7 147. Defendants performed these acts for the purpose of secretly collecting Ms.
8 Hong’s private and personally-identifiable data and content – including her User/Device
9 Identifiers, biometric identifiers and information, and Private Videos – and using such data
10 and content to track, profile and target Ms. Hong with advertisements. Further, Defendants
11 have used Ms. Hong’s private and personally-identifiable data and content for the purpose
12 of developing their artificial intelligence capabilities and patenting commercially-valuable
13 technologies. Defendants and others now have access to a living and information-laden
14 dossier on Ms. Hong that can be used for further commercial advantage and other harmful
15 purposes. Defendants have profited, and will continue to profit, from these activities.

16 148. Meanwhile, Ms. Hong has incurred harm as a result of Defendants’ invasion
17 of her privacy rights through their covert taking of her private and personally-identifiable
18 data and content – including her User/Device Identifiers, biometric identifiers and
19 information, and Private Videos. Ms. Hong also has suffered harm because Defendant’s
20 actions have diminished the value of her private and personally-identifiable data and
21 content. Moreover, Ms. Hong has suffered injury to her mobile device. The battery,
22 memory, CPU and bandwidth of her device has been compromised, and as a result the
23 functioning of that device has been impaired and slowed, due to Defendants’ clandestine
24 and unlawful activities. Finally, Ms. Hong has incurred additional data usage and
25 electricity costs that she would not have incurred but for Defendants’ covert and unlawful
26 actions.

27 2. **Plaintiff A.S.**

28 149. Plaintiff A.S., a minor who is currently 15 years old, first downloaded the

1 Musical.ly app to her mobile device and created a user account in 2016 when she was
 2 under age 13. She subsequently downloaded the Musical.ly app in 2017 to a new mobile
 3 device that was hers. In 2019, A.S. downloaded the TikTok app to another new mobile
 4 device that was hers. A.S. and her legal guardian have never seen or read any of
 5 Defendants' privacy policies or terms of use.

6 150. Beginning in 2016, A.S. created numerous videos using the Musical.ly app
 7 and the TikTok app. Many are Private Videos containing images of her face, while many
 8 others are videos containing her voice and images of her face that she intentionally
 9 uploaded and posted. A.S. used the augmented reality features and facial filters on her face
 10 in both Private Videos and in videos that she intentionally uploaded and posted.

11 151. During the time that the TikTok app was installed on A.S.'s mobile devices,
 12 Defendants surreptitiously performed the following actions without notice to or the
 13 knowledge and consent of A.S. or her legal guardian: (i) Defendants took her User/Device
 14 Identifiers, Private Videos and Private Video Images from her mobile devices; (ii)
 15 Defendants took her biometric identifiers and information (including face geometry scans
 16 and voiceprints) from her mobile devices and/or videos; (iii) Defendants took her private
 17 and personally-identifiable data and content from her other social media accounts; (iv)
 18 Defendants took her private and personally-identifiable data and content from her mobile
 19 devices before she had the opportunity to sign up and create an account; (v) Defendants
 20 took her private and personally-identifiable data and content from her mobile devices after
 21 she closed the TikTok app; and (vi) Defendants transferred some or all such stolen data
 22 and content to servers located in China – including to servers under the control of third-
 23 parties who cooperate with the Chinese government.

24 152. Defendants performed these acts for the purpose of secretly collecting A.S.'s
 25 private and personally-identifiable data and content – including her User/Device
 26 Identifiers, biometric identifiers and information, Private Videos and Private Video Images
 27 – and using such data and content to track, profile and target A.S. with advertisements.
 28 Further, Defendants have used A.S.'s private and personally-identifiable data and content

1 for the purpose of developing their artificial intelligence capabilities and patenting
2 commercially-valuable technologies. Defendants and others now have access to a living
3 and information-laden dossier on A.S. that can be used for further commercial advantage
4 and other harmful purposes. Defendants have profited, and will continue to profit, from
5 these activities.

6 153. Meanwhile, A.S. has incurred harm as a result of Defendants' invasion of her
7 privacy rights through their covert taking of her private and personally-identifiable data
8 and content – including her User/Device Identifiers, biometric identifiers and information,
9 Private Videos and Private Video Images. A.S. also has suffered harm because
10 Defendant's actions have diminished the value of her private and personally-identifiable
11 data and content. Moreover, A.S. has suffered injury to her mobile devices. The battery,
12 memory, CPU and bandwidth of such devices have been compromised, and as a result the
13 functioning of those devices has been impaired and slowed, due to Defendants' clandestine
14 and unlawful activities. Finally, A.S. has incurred additional data usage and electricity
15 costs that she would not have incurred but for Defendants' covert and unlawful actions.

16 **3. Plaintiff A.R.**

17 154. A.R. downloaded the Musical.ly app to her mobile device and created a user
18 account in or about 2017 when she was approximately 12 years old. Subsequently, in
19 2019, while still a minor, A.R. downloaded the TikTok app to a new mobile device that
20 was hers. A.R. and her legal guardian have never seen or read any of Defendants' privacy
21 policies or terms of use.

22 155. A.R. created numerous videos using the Musical.ly app and the TikTok app.
23 Many are Private Videos containing images of her face, while many others are videos
24 containing images of her face that she intentionally uploaded and posted. A.R. used the
25 augmented reality features and facial filters on her face in her Private Videos. A.R.'s voice
26 and images of A.R.'s face have been captured in Private Videos recorded by others, as well
27 as in videos that were recorded, uploaded and posted by others.

28 156. During the time that the TikTok app was installed on A.R.'s mobile devices,

1 Defendants surreptitiously performed the following actions without notice to or the
2 knowledge and consent of A.R. or her legal guardian: (i) Defendants took her User/Device
3 Identifiers, Private Videos and Private Video Images from her mobile devices; (ii)
4 Defendants took her biometric identifiers and information (including face geometry scans
5 and voiceprints) from her and her friends' mobile devices and/or videos; (iii) Defendants
6 took her private and personally-identifiable data and content from her mobile devices
7 before she had the opportunity to sign up and create an account; (iv) Defendants took her
8 private and personally-identifiable data and content from her mobile devices after she
9 closed the TikTok app; and (v) Defendants transferred some or all such stolen data and
10 content to servers located in China – including to servers under the control of third-parties
11 who cooperate with the Chinese government.

12 157. Defendants performed these acts for the purpose of secretly collecting A.R.'s
13 private and personally-identifiable data and content – including her User/Device
14 Identifiers, biometric identifiers and information, Private Videos and Private Video Images
15 – and using such data and content to track, profile and target A.R. with advertisements.
16 Further, Defendants have used A.R.'s private and personally-identifiable data and content
17 for the purpose of developing their artificial intelligence capabilities and patenting
18 commercially-valuable technologies. Defendants and others now have access to a living
19 and information-laden dossier on A.R. that can be used for further commercial advantage
20 and other harmful purposes. Defendants have profited, and will continue to profit, from
21 these activities.

22 158. Meanwhile, A.R. has incurred harm as a result of Defendants' invasion of
23 her privacy rights through their covert taking of her private and personally-identifiable data
24 and content – including her User/Device Identifiers, biometric identifiers and information,
25 Private Videos and Private Video Images. A.R. also has suffered harm because
26 Defendant's actions have diminished the value of her private and personally-identifiable
27 data and content. Moreover, A.R. has suffered injury to her mobile devices. The battery,
28 memory, CPU and bandwidth of her devices have been compromised, and as a result the

1 functioning of those devices has been impaired and slowed, due to Defendants' clandestine
 2 and unlawful activities. Finally, A.R. has incurred additional data usage and electricity
 3 costs that she would not have incurred but for Defendants' covert and unlawful actions.

4 **B. The Illinois Plaintiffs.**

5 **1. Plaintiff Meghan Smith.**

6 159. Plaintiff Meghan Smith downloaded the TikTok app to her mobile device
 7 and created a user account in 2018. Ms. Smith has never read and does not recall seeing
 8 any of Defendants' privacy policies or terms of use.

9 160. Ms. Smith created numerous videos using the TikTok app. Many are Private
 10 Videos containing her voice and images of her face, while many others are videos
 11 containing her voice and images of her face that she intentionally uploaded and posted.
 12 Ms. Smith used the augmented reality features and facial filters on her face in both Private
 13 Videos and in videos that she intentionally uploaded and posted.

14 161. During the time that the TikTok app was installed on Ms. Smith's mobile
 15 device, Defendants surreptitiously performed the following actions without notice to or the
 16 knowledge and consent of Ms. Smith: (i) Defendants took her User/Device Identifiers,
 17 Private Videos, and Private Video Images from her mobile device; (ii) Defendants took her
 18 biometric identifiers and information (including face geometry scans and voiceprints) from
 19 her mobile device and/or videos; (iii) Defendants took her private and personally-
 20 identifiable data and content from her mobile device before she had the opportunity to sign
 21 up and create an account; (iv) Defendants took her private and personally-identifiable data
 22 and content from her mobile device after she closed the TikTok app; and (v) Defendants
 23 transferred some or all such stolen data and content to servers located in China – including
 24 to servers under the control of third-parties who cooperate with the Chinese government.

25 162. Defendants performed these acts for the purpose of secretly collecting Ms.
 26 Smith's private and personally-identifiable data and content – including her User/Device
 27 Identifiers, biometric identifiers and information, Private Videos and Private Video Images
 28 – and using such data and content to track, profile and target Ms. Smith with

1 advertisements. Further, Defendants have used Ms. Smith's private and personally-
 2 identifiable data and content for the purpose of developing their artificial intelligence
 3 capabilities and patenting commercially-valuable technologies. Defendants and others now
 4 have access to a living and information-laden dossier on Ms. Smith that can be used for
 5 further commercial advantage and other harmful purposes. Defendants have profited, and
 6 will continue to profit, from these activities.

7 163. Meanwhile, Ms. Smith has incurred harm as a result of Defendants' invasion
 8 of her privacy rights through their covert taking of her private and personally-identifiable
 9 data and content – including her User/Device Identifiers, biometric identifiers and
 10 information, Private Videos and Private Video Images. Ms. Smith also has suffered harm
 11 because Defendant's actions have diminished the value of her private and personally-
 12 identifiable data and content. Moreover, Ms. Smith has suffered injury to her mobile
 13 device. The battery, memory, CPU and bandwidth of such device have been compromised,
 14 and as a result the functioning of that device has been impaired and slowed, due to
 15 Defendants' clandestine and unlawful activities. Finally, Ms. Smith has incurred additional
 16 data usage and electricity costs that she would not have incurred but for Defendants' covert
 17 and unlawful actions.

18 2. Plaintiffs C.W. and I.W.

19 164. Plaintiff C.W., a minor who is currently 11 years old, and Plaintiff I.W., a
 20 minor who is currently 8 years old, are siblings who each downloaded the TikTok app to
 21 their own mobile devices and created their respective user accounts in or about March
 22 2019. C.W., I.W. and their legal guardian have never seen or read any of Defendants'
 23 privacy policies or terms of use.

24 165. C.W. and I.W. each created numerous videos using the TikTok app. Each
 25 has videos containing images of their respective faces that they intentionally uploaded and
 26 posted. C.W. and I.W. used the augmented reality features and facial filters on their
 27 respective faces in videos they intentionally uploaded and posted.

28 166. During the time that the TikTok app was installed on C.W.'s and I.W.'s

1 mobile devices, Defendants surreptitiously performed the following actions without notice
2 to or the knowledge and consent of C.W., I.W., or their legal guardian: (i) Defendants took
3 their User/Device Identifiers from their mobile devices; (ii) Defendants took their
4 biometric identifiers and information (including face geometry scans and voiceprints) from
5 their mobile device and/or videos; (iii) Defendants took their private and personally-
6 identifiable data and content from their mobile devices before they had the opportunity to
7 sign up and create an account; (iv) Defendants took their private and personally-
8 identifiable data and content from their mobile devices after they closed the TikTok app;
9 and (v) Defendants transferred some or all such stolen data and content to servers located
10 in China – including to servers under the control of third-parties who cooperate with the
11 Chinese government.

12 167. Defendants performed these acts for the purpose of secretly collecting
13 C.W.’s and I.W.’s private and personally-identifiable data and content – including their
14 User/Device Identifiers and biometric identifiers and information – and using such data
15 and content to track, profile and target C.W. and I.W. with advertisements. Further,
16 Defendants have used C.W.’s and I.W.’s private and personally-identifiable data and
17 content for the purpose of developing Defendants’ artificial intelligence capabilities and
18 patenting commercially-valuable technologies. Defendants and others now have access to
19 a living and information-laden dossier on C.W. and I.W. that can be used for further
20 commercial advantage and other harmful purposes. Defendants have profited, and will
21 continue to profit, from these activities.

22 168. Meanwhile, C.W. and I.W. have incurred harm as a result of Defendants’
23 invasion of their privacy rights through Defendants’ covert taking of C.W.’s and I.W.’s
24 private and personally-identifiable data and content – including their User/Device
25 Identifiers and biometric identifiers and information. C.W. and I.W. also have suffered
26 harm because Defendant’s actions have diminished the value of their private and
27 personally-identifiable data and content. Moreover, C.W. and I.W. have suffered injury to
28 their mobile devices. The battery, memory, CPU and bandwidth of such devices have been

1 compromised, and as a result the functioning of those devices has been impaired and
 2 slowed, due to Defendants' clandestine and unlawful activities. Finally, C.W. and I.W.
 3 have incurred additional data usage and electricity costs that they would not have incurred
 4 but for Defendants' covert and unlawful actions.

5 **3. Plaintiff R.P.**

6 169. R.P., a minor who is currently 11 years old, downloaded the TikTok app to
 7 her mobile device and created a user account in 2018. R.P. and her legal guardian have
 8 never seen or read any of Defendants' privacy policies or terms of use.

9 170. R.P. created numerous videos using the TikTok app. Many are Private
 10 Videos containing images of her face, while many others are videos containing images of
 11 her face that she intentionally uploaded and posted. R.P. used the augmented reality
 12 features and facial filters on her face in both Private Videos and in videos that she
 13 intentionally uploaded and posted. Images of R.P.'s face have been captured in videos that
 14 were recorded, uploaded and posted by others.

15 171. During the time that the TikTok app was installed on R.P.'s mobile device,
 16 Defendants surreptitiously performed the following actions without notice to or the
 17 knowledge and consent of R.P. or her legal guardian: (i) Defendants took her User/Device
 18 Identifiers, Private Videos and Private Video Images from her mobile device; (ii)
 19 Defendants took her biometric identifiers and information (including face geometry scans
 20 and voiceprints) from her mobile device and/or videos; (iii) Defendants took her private
 21 and personally-identifiable data and content from her mobile device before she had the
 22 opportunity to sign up and create an account; (iv) Defendants took her private and
 23 personally-identifiable data and content from her mobile device after she closed the
 24 TikTok app; and (v) Defendants transferred some or all such stolen data and content to
 25 servers located in China – including to servers under the control of third-parties who
 26 cooperate with the Chinese government.

27 172. Defendants performed these acts for the purpose of secretly collecting R.P.'s
 28 private and personally-identifiable data and content – including her User/Device

Identifiers, biometric identifiers and information, and Private Videos and Private Video Images – and using such data and content to track, profile and target R.P. with advertisements. Further, Defendants have used R.P.’s private and personally-identifiable data and content for the purpose of developing their artificial intelligence capabilities and patenting commercially-valuable technologies. Defendants and others now have access to a living and information-laden dossier on R.P. that can be used for further commercial advantage and other harmful purposes. Defendants have profited, and will continue to profit, from these activities.

173. Meanwhile, R.P. has incurred harm as a result of Defendants’ invasion of her privacy rights through their covert taking of her private and personally-identifiable data and content – including her User/Device Identifiers, biometric identifiers and information, and Private Videos and Private Video Images. R.P. also has suffered harm because Defendant’s actions have diminished the value of her private and personally-identifiable data and content. Moreover, R.P. has suffered injury to her mobile device. The battery, memory, CPU and bandwidth of her device have been compromised, and as a result the functioning of that device has been impaired and slowed, due to Defendants’ clandestine and unlawful activities. Finally, R.P. has incurred additional data usage and electricity costs that she would not have incurred but for Defendants’ covert and unlawful actions.

X. CLASS ALLEGATIONS.

174. Plaintiffs seek class certification of the class set forth herein pursuant to Federal Rule of Civil Procedure 23 (“Rule 23”). Specifically, Plaintiffs seek class certification of all claims for relief herein on behalf of a class and two subclasses defined as follows:

Class: All persons who used the TikTok app and/or the Musical.ly app on one or more of their mobile devices while residing in the United States.

California Subclass: All persons who used the TikTok app and/or the Musical.ly app on one or more of their mobile devices while residing in California.

Illinois Subclass: All persons who, while residing in Illinois, used the TikTok app

1 and/or the Musical.ly app on one or more of their mobile devices and who, while residing
 2 in Illinois, (i) used either app to make a video containing his or her own face and/or voice,
 3 and/or (ii) had his or her own face and/or voice captured in a video made by someone else
 4 with either app.

5 175. Plaintiffs are the proposed class representatives for the class. California
 6 Plaintiffs are the proposed class representatives for the California Subclass. Illinois
 7 Plaintiffs are the proposed class representatives for the Illinois Subclass.

8 176. Plaintiffs reserve the right to modify or refine the definitions of the Class and
 9 the two Subclasses based upon discovery of new information and in order to accommodate
 10 any of the Court's manageability concerns.

11 177. Excluded from the Class and the two Subclasses are: (i) any judge or
 12 magistrate judge presiding over this action and members of their staff, as well as members
 13 of their families; (ii) Defendants, Defendants' predecessors, parents, successors, heirs,
 14 assigns, subsidiaries, and any entity in which any Defendant or its parents have a
 15 controlling interest, as well as Defendants' current or former employees, agents, officers,
 16 and directors; (iii) persons who properly execute and file a timely request for exclusion
 17 from the class; (iv) persons whose claims in this matter have been finally adjudicated on
 18 the merits or otherwise released; (v) counsel for Plaintiffs and Defendants; and (vi) the
 19 legal representatives, successors, and assigns of any such excluded persons.

20 178. **Ascertainability.** The proposed Class and Subclasses are readily
 21 ascertainable because they are defined using objective criteria so as to allow Class and
 22 Subclass members to determine if they are part of the Class and/or one of the two
 23 Subclasses. Further, the Class and two Subclasses can be readily identified through records
 24 maintained by Defendants.

25 179. **Numerosity (Rule 23(a)(1)).** The Class and two Subclasses are so numerous
 26 that joinder of individual members herein is impracticable. The exact number of Class and
 27 Subclass members, as herein identified and described, is not known, but download figures
 28 indicate that the TikTok app has been downloaded more than 120 million times in the

1 United States.

2 180. **Commonality (Rule 23(a)(2)).** Common questions of fact and law exist for
3 each cause of action and predominate over questions affecting only individual Class and
4 Subclass members, including the following:

5 a. Whether Defendants engaged in the activities and practices referenced
6 above;

7 b. Whether Defendants' activities and practices referenced above
8 constitute a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030;

9 c. Whether Defendants' activities and practices referenced above
10 constitute a violation of the California Comprehensive Data Access and Fraud Act, Cal.
11 Pen. C. § 502;

12 d. Whether Defendants' activities and practices referenced above
13 constitute a violation of the Right to Privacy under the California Constitution;

14 e. Whether Defendants' activities and practices referenced above
15 constitute an intrusion upon seclusion;

16 f. Whether Defendants' activities and practices referenced above
17 constitute a violation of the California Unfair Competition Law, Bus. & Prof. C. §§ 17200
18 *et seq.*

19 g. Whether Defendants' activities and practices referenced above
20 constitute a violation of the California False Advertising Law, Bus. & Prof. C. §§ 17500 *et*
21 *seq.*

22 h. Whether Defendants' activities and practices referenced above
23 constitute negligence;

24 i. Whether Defendants' activities and practices referenced above
25 constitute unjust enrichment concerning which restitution and/or disgorgement is
26 warranted;

27 j. Whether Defendants' activities and practices referenced above
28 constitute a violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et*

1 *seq.*;

2 k. Whether Plaintiffs and members of the Class and two Subclasses
3 sustained damages as a result of Defendants' activities and practices referenced above,
4 and, if so, in what amount;

5 l. Whether Defendants profited from their activities and practices
6 referenced above, and, if so, in what amount;

7 m. What is the appropriate injunctive relief to ensure that Defendants no
8 longer unlawfully: **(i)** take private and personally-identifiable TikTok user data and content
9 – including User/Device Identifiers, biometric identifiers and information, and Private
10 Videos and Private Video Images; **(ii)** utilize private and personally-identifiable TikTok
11 user data and content to develop and patent commercially-valuable artificial intelligence
12 technologies; **(iii)** utilize private and personally-identifiable TikTok user data and content
13 to create consumer demand for and use of Defendants' other products; **(iv)** transfer such
14 private and personally-identifiable TikTok user data and content to servers in China and to
15 third parties either in China or whose data is accessible from within China; **(v)** cause the
16 diminution in value of TikTok users' private and personally-identifiable data and content;
17 **(vi)** cause injury and harm to TikTok users' mobile devices; **(vii)** cause TikTok users to
18 incur higher data usage and electricity charges; **(viii)** retain the unlawfully assembled
19 TikTok user dossiers, including all private and personally-identifiable data and content
20 therein; and **(ix)** profile and target, based on the above activities, TikTok users with
21 advertisements.

22 n. What is the appropriate injunctive relief to ensure that Defendants
23 take reasonable measures to ensure that they and relevant third parties destroy unlawfully-
24 acquired private and personally-identifiable TikTok user data and content in their
25 possession, custody or control.

26 181. **Typicality (Rule 23(a)(3)).** Plaintiffs' claims are typical of the claims of
27 members of the Class and two Subclasses because, among other things, Plaintiffs and
28 members of the Class and two Subclasses sustained similar injuries as a result of

1 Defendants' uniform wrongful conduct and their legal claims all arise from the same
2 events and wrongful conduct by Defendants.

3 182. **Adequacy (Rule 23(a)(4)).** Plaintiffs will fairly and adequately protect the
4 interests of the Class and two Subclasses. Plaintiffs' interests do not conflict with the
5 interests of the Class and Subclass members, and Plaintiffs have retained counsel
6 experienced in complex class action and data privacy litigation to prosecute this case on
7 behalf of the Class and two Subclasses.

8 183. **Predominance & Superiority (Rule 23(b)(3)).** In addition to satisfying the
9 prerequisites of Rule 23(a), Plaintiffs satisfy the requirements for maintaining a class
10 action under Rule 23(b)(3). Common questions of law and fact predominate over any
11 questions affecting only individual Class and Subclass members, and a class action is
12 superior to individual litigation and all other available methods for the fair and efficient
13 adjudication of this controversy. The amount of damages available to Plaintiffs is
14 insufficient to make litigation addressing Defendants' conduct economically feasible in the
15 absence of the class action procedure. Individualized litigation also presents a potential for
16 inconsistent or contradictory judgments, and increases the delay and expense presented by
17 the complex legal and factual issues of the case to all parties and the court system. By
18 contrast, the class action device presents far fewer management difficulties and provides
19 the benefits of a single adjudication, economy of scale, and comprehensive supervision by
20 a single court.

21 184. **Final Declaratory or Injunctive Relief (Rule 23(b)(2)).** Plaintiffs also
22 satisfy the requirements for maintaining a class action under Rule 23(b)(2). Defendants
23 have acted or refused to act on grounds that apply generally to the Class and two
24 Subclasses, making final declaratory and/or injunctive relief appropriate with respect to the
25 Class and two Subclasses as a whole.

26 185. **Particular Issues (Rule 23(c)(4)).** Plaintiffs also satisfy the requirements for
27 maintaining a class action under Rule 23(c)(4). Their claims consist of particular issues
28 that are common to all Class and Subclass members and are capable of class-wide

1 resolution that will significantly advance the litigation.

2 **XI. CAUSES OF ACTION.**

3 **FIRST CAUSE OF ACTION**

4 **Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030**

5 **(On Behalf of the Plaintiffs and the Class)**

6 186. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if
7 fully set forth herein.

8 187. The Plaintiffs’ and the Class’s mobile devices are, and at all relevant times
9 have been, used for interstate communication and commerce, and are therefore “protected
10 computers” under 18 U.S.C. § 1030(e)(2)(B).

11 188. Defendants have exceeded, and continue to exceed, authorized access to the
12 Plaintiffs’ and the Class’s protected computers and obtained information thereby, in
13 violation of 18 U.S.C. § 1030(a)(2), (a)(2)(C).

14 189. Defendants’ conduct caused “loss to 1 or more persons during any 1-year
15 period . . . aggregating at least \$5,000 in value” under 18 U.S.C. § 1030(c)(4)(A)(i)(I),
16 *inter alia*, because of the secret transmission of the Plaintiffs’ and the Class’s private and
17 personally-identifiable data and content – including User/Device Identifiers, biometric
18 identifiers and information, and Private Videos and Private Video Images never intended
19 for public consumption.

20 190. Defendants’ conduct also constitutes “a threat to public health or safety”
21 under 18 U.S.C. § 1030(c)(4)(A)(i)(IV), due to the private and personally-identifiable data
22 and content of the Plaintiffs and the Class being made available to foreign actors, including
23 foreign intelligence services, in locations without adequate legal privacy protections. That
24 this threat is real and imminent is evidenced by the ban on the TikTok app instituted by the
25 Defense Department, Navy, Army, Marines, Air Force, Coast Guard and Transportation
26 Security Administration, as well as the proposed legislation by United States Senators that
27 would ban federal employees from using the TikTok app. As Senators Schumer and Cotton
28 wrote in an October 23, 2019 letter to the Acting Director of National Intelligence

1 concerning TikTok, “[s]ecurity experts have voiced concerns that China’s vague
 2 patchwork of intelligence, national security, and cybersecurity laws compel Chinese
 3 companies to support and cooperate with intelligence work controlled by the Chinese
 4 Communist Party. Without an independent judiciary to review requests made by the
 5 Chinese government for data or other actions, there is no legal mechanism for Chinese
 6 companies to appeal if they disagree with a request.”¹³⁴

7 191. Accordingly, the Plaintiffs and the Class are entitled to “maintain a civil
 8 action against the violator to obtain compensatory damages and injunctive relief or other
 9 equitable relief.” 18 U.S.C. § 1030(g).

10 **SECOND CAUSE OF ACTION**

11 **Violation of the California Comprehensive** 12 **Data Access and Fraud Act, Cal. Pen. C. § 502** 13 **(On Behalf of the Plaintiffs and the Class)**

14 192. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if
 15 fully set forth herein.

16 193. Defendants’ acts violate Cal. Pen. C. § 502(c)(1) because they have
 17 knowingly accessed, and continue to knowingly access, data and computers to wrongfully
 18 control or obtain data. The Plaintiffs’ and the Class’s private and personally-identifiable
 19 data and content accessed by Defendants – including the User/Device Identifiers, the
 20 biometric identifiers and information, and the Private Videos and Private Video Images
 21 never intended for public consumption – far exceeds any reasonable use of the Plaintiffs’
 22 and the Class’s data and content to operate the TikTok app. There is no justification for
 23 Defendants’ surreptitious collection and transfer of the Plaintiffs’ and the Class’s private
 24 and personally-identifiable data and content from their mobile devices and their other
 25 social media accounts; for Defendants’ clandestine collection and transfer of the Plaintiffs’
 26

27 ¹³⁴ [https://www.law360.com/articles/1213180/sens-want-tiktok-investigated-for-national-security-](https://www.law360.com/articles/1213180/sens-want-tiktok-investigated-for-national-security-threats)
 28 [threats; https://www.cotton.senate.gov/?p=press_release&id=1239.](https://www.cotton.senate.gov/?p=press_release&id=1239)

1 and the Class's private and personally-identifiable data and content before they even sign-
2 up and create an account; for Defendants' covert collection and transfer of the Plaintiffs'
3 and the Class's private and personally-identifiable data and content when the TikTok app
4 is closed; or for Defendants having embedded source code within the TikTok app that
5 transfers the Plaintiffs' and the Class's private and personally-identifiable data and content
6 to servers and third-party companies based in China where such servers and third-party
7 companies are subject to Chinese law requiring the sharing of such data and content with
8 the Chinese government.

9 194. Defendants' acts violate Cal. Pen. C. § 502(c)(2) because they have
10 knowingly accessed and without permission taken, copied, and made use of data from a
11 computer – and they continue to do so. Defendants did not obtain permission to take, copy,
12 and make use of the Plaintiffs' and the Class's private and personally-identifiable data and
13 content – including the User/Device Identifiers, biometric identifiers and information, and
14 Private Videos and Private Video Images never intended for public consumption – from
15 their mobile devices and their other social media accounts. Nor did Defendants obtain
16 permission to take, copy, and make use of the Plaintiffs' and the Class's private and
17 personally-identifiable data and content from their mobile devices before they even sign-
18 up and create an account. And Defendants did not obtain permission to take, copy, and
19 make use of the Plaintiffs' and the Class's private and personally-identifiable data and
20 content from their mobile devices when the TikTok app is closed. Finally, Defendants did
21 not obtain permission to embed source code within the TikTok app that transfers the
22 Plaintiffs' and the Class's private and personally-identifiable data and content to servers
23 and third-party companies based in China where such servers and third-party companies
24 are subject to Chinese law requiring the sharing of such data and content with the Chinese
25 government.

26 195. Accordingly, the Plaintiffs and the Class are entitled to compensatory
27 damages, including “any expenditure reasonably and necessarily incurred by the owner or
28 lessee to verify that a computer system, computer network, computer program, or data was

1 or was not altered, damaged, or deleted by the access,” injunctive relief, and attorneys’
2 fees. Cal. Pen. C. § 502(e)(1), (2).

3 **THIRD CAUSE OF ACTION**

4 **Violation of the Right to Privacy – California Constitution**

5 **(On Behalf of the California Plaintiffs and the California Subclass)**

6 196. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if
7 fully set forth herein.

8 197. The California Plaintiffs and the California Subclass hold, and at all relevant
9 times held, a legally protected privacy interest in their private and personally-identifiable
10 data and content – including the User/Device Identifiers, the biometric identifiers and
11 information, and the Private Videos and Private Video Images never intended for public
12 consumption – on their mobile devices and in their other social media accounts that
13 Defendants have taken.

14 198. There is a reasonable expectation of privacy concerning the California
15 Plaintiffs’ and the California Subclass’s data and content under the circumstances present.

16 199. The reasonableness of the California Plaintiffs’ and the California Subclass’s
17 expectation of privacy is supported by the undisclosed, hidden, and non-intuitive nature of
18 Defendants’ taking of private and personally-identifiable data and content – including the
19 User/Device Identifiers, the biometric identifiers and information, and the Private Videos
20 and Private Video Images never intended for public consumption – from the California
21 Plaintiffs’ and the California Subclass’s mobile devices and other social media accounts.

22 200. Defendants’ conduct constitutes and, at all relevant times, constituted a
23 serious invasion of privacy, as Defendants either did not disclose at all, or failed to make
24 an effective disclosure, that they would take and make use of – and allow third-party
25 companies based in China to take and make use of – the California Plaintiffs’ and the
26 California Subclass’s private and personally-identifiable data and content. Defendants
27 intentionally invaded the California Plaintiffs’ and the California Subclass’s privacy
28 interests by intentionally designing the TikTok app, including all associated code, to

1 surreptitiously obtain, improperly gain knowledge of, review, and retain their private and
2 personally-identifiable data and content.

3 201. These intrusions are highly offensive to a reasonable person, as evidenced by
4 substantial research, literature, and governmental enforcement and investigative efforts to
5 protect consumer privacy against surreptitious technological intrusions. The offensiveness
6 of Defendants' intrusion is heightened by Defendants' making the California Plaintiffs'
7 and the California Subclass's private and personally-identifiable data and content available
8 to third parties, including foreign governmental entities whose interests are opposed to
9 those of United States citizens. The offensiveness of Defendants' intrusion is further
10 heightened by Defendants' secret collection and transfer of the California Plaintiffs' and
11 the California Subclass's private and personally-identifiable data and content before they
12 even sign-up and create an account; by Defendants' covert collection and transfer of the
13 California Plaintiffs' and the California Subclass's private and personally-identifiable data
14 and content when the TikTok app is closed; and by Defendants' clandestine collection and
15 transfer of the California Plaintiffs' and the California Subclass's private and personally-
16 identifiable data and content from their other social media accounts. The intentionality of
17 Defendants' conduct, and the steps they have taken to disguise and deny it, also
18 demonstrate the highly offensive nature of their conduct. Further, Defendants' conduct
19 targeted the California Plaintiffs' and the California Subclass's mobile devices, which the
20 United States Supreme Court has characterized as almost a feature of human anatomy, and
21 which contain the California Plaintiffs' and the California Subclass's private and
22 personally-identifiable data and content.

23 202. The California Plaintiffs and the California Subclass were harmed by, and
24 continue to suffer harm as a result of, the intrusion as detailed throughout this First
25 Amended Complaint.

26 203. Defendants' conduct was a substantial factor in causing the harm suffered by
27 the California Plaintiffs and the California Subclass.

28 204. The California Plaintiffs and the California Subclass seek nominal and

1 punitive damages as a result of Defendants' actions. Punitive damages are warranted
2 because Defendants' malicious, oppressive, and willful actions were calculated to injure
3 the California Plaintiffs and the California Subclass, and were made in conscious disregard
4 of their rights. Punitive damages are also warranted to deter Defendants from engaging in
5 future misconduct.

6 205. The California Plaintiffs and the California Subclass seek injunctive relief to
7 rectify Defendants' actions, including but not limited to requiring Defendants to stop
8 taking more private and personally-identifiable data and content of the California Plaintiffs
9 and the California Subclass from their mobile devices and their other social media
10 accounts than is reasonably necessary to operate the TikTok app; to make clear disclosures
11 of the California Plaintiffs' and the California Subclass's private and personally-
12 identifiable data and content that is reasonably necessary to operate the TikTok app; to
13 obtain the California Plaintiffs' and the California Subclass's consent to the taking of their
14 private and personally-identifiable data and content; to stop transferring the California
15 Plaintiffs' and the California Subclass's private and personally-identifiable data and
16 content to China, to servers located in China, or to servers or companies whose data is
17 accessible from within China; and to recall and destroy the California Plaintiffs' and the
18 California Subclass's private and personally-identifiable data and content already taken in
19 contravention of the California Plaintiffs' and the California Subclass's right to privacy
20 under the California Constitution.

21 206. The California Plaintiffs and the California Subclass seek restitution and
22 disgorgement for Defendants' violation of their privacy rights. A person acting in
23 conscious disregard of the rights of another is required to disgorge all profit because
24 disgorgement both benefits the injured parties and deters the perpetrator from committing
25 the same unlawful actions again. Disgorgement is available for conduct that constitutes
26 "conscious interference with a claimant's legally protected interests," including tortious
27 conduct or conduct that violates another duty or prohibition. Restatement (3rd) of
28 Restitution and Unjust Enrichment, §§ 40, 44.

FOURTH CAUSE OF ACTION

Intrusion upon Seclusion

(On Behalf of the Plaintiffs and the Class)

207. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

208. “One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.” Restatement (2nd) of Torts § 652B.

209. The Plaintiffs and the Class have, and at all relevant times had, a reasonable expectation of privacy in their mobile devices and their other social media accounts, and their private affairs include their past, present and future activity on their mobile devices and their other social media accounts.

210. The reasonableness of the Plaintiffs’ and the Class’s expectations of privacy is supported by the undisclosed, hidden, and non-intuitive nature of Defendants’ taking of private and personally-identifiable data and content from the Plaintiffs’ and the Class’s mobile devices and other social media accounts.

211. Defendants intentionally intruded upon the Plaintiffs’ and the Class’s solitude, seclusion, and private affairs – and continue to do so – by intentionally designing the TikTok app, including all associated code, to surreptitiously obtain, improperly gain knowledge of, review, and retain the Plaintiffs’ and the Class’s private and personally-identifiable data and content – including the User/Device Identifiers, the biometric identifiers and information, and the Private Videos and Private Video Images never intended for public consumption.

212. These intrusions are highly offensive to a reasonable person, as evidenced by substantial research, literature, and governmental enforcement and investigative efforts to protect consumer privacy against surreptitious technological intrusions. The offensiveness of Defendants’ intrusion is heightened by Defendants’ making the Plaintiffs’ and the

1 Class's private and personally-identifiable data and content available to third parties,
2 including foreign governmental entities whose interests are opposed to those of United
3 States citizens. The offensiveness of Defendants' intrusion is further heightened by
4 Defendants' secret collection and transfer of the Plaintiffs' and the Class's private and
5 personally-identifiable data and content before they even sign-up and create an account; by
6 Defendants' covert collection and transfer of the Plaintiffs' and the Class's private and
7 personally-identifiable data and content when the TikTok app is closed; and by
8 Defendants' clandestine collection and transfer of the Plaintiffs' and the Class's private
9 and personally-identifiable data and content from their other social media accounts. The
10 intentionality of Defendants' conduct, and the steps they have taken to disguise and deny
11 it, also demonstrate the highly offensive nature of their conduct. Further, Defendants'
12 conduct targeted the Plaintiffs' and the Class's mobile devices, which the United States
13 Supreme Court has characterized as almost a feature of human anatomy, and which contain
14 the Plaintiffs' and the Class's private and personally-identifiable data and content.

15 213. The Plaintiffs and the Class were harmed by, and continue to suffer harm as
16 a result of, the intrusion as detailed throughout this First Amended Complaint.

17 214. Defendants' conduct was a substantial factor in causing the harm suffered by
18 the Plaintiffs and the Class.

19 215. The Plaintiffs and the Class seek nominal and punitive damages as a result of
20 Defendants' actions. Punitive damages are warranted because Defendants' malicious,
21 oppressive, and willful actions were calculated to injure the Plaintiffs and the Class, and
22 were made in conscious disregard of their rights. Punitive damages are also warranted to
23 deter Defendants from engaging in future misconduct.

24 216. The Plaintiffs and the Class seek injunctive relief to rectify Defendants'
25 actions, including but not limited to requiring Defendants to stop taking more private and
26 personally-identifiable data and content from the Plaintiffs' and the Class's mobile devices
27 and other social media accounts than is reasonably necessary to operate the TikTok app; to
28 make clear disclosures of the Plaintiffs' and the Class's private and personally-identifiable

1 data and content that is reasonably necessary to operate the TikTok app; to obtain the
 2 Plaintiffs' and the Class's consent to the taking of such private and personally-identifiable
 3 data and content; to stop transferring the Plaintiffs' and the Class's private and personally-
 4 identifiable data and content to China, to servers located in China, or to servers or
 5 companies whose data is accessible from within China; and to recall and destroy the
 6 Plaintiffs' and the Class's private and personally-identifiable data and content already
 7 taken in contravention of the Plaintiffs' and the Class's privacy rights.

8 217. Plaintiffs and the Class seek restitution and disgorgement for Defendants'
 9 intrusion upon seclusion. A person acting in conscious disregard of the rights of another is
 10 required to disgorge all profit because disgorgement both benefits the injured parties and
 11 deters the perpetrator from committing the same unlawful actions again. Disgorgement is
 12 available for conduct that constitutes "conscious interference with a claimant's legally
 13 protected interests," including tortious conduct or conduct that violates another duty or
 14 prohibition. Restatement (3rd) of Restitution and Unjust Enrichment, §§ 40, 44.

15 **FIFTH CAUSE OF ACTION**

16 **Violation of the California Unfair Competition Law,**

17 **Bus. & Prof. C. §§ 17200 et seq.**

18 **(On Behalf of the Plaintiffs and the Class)**

19 218. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if
 20 fully set forth herein.

21 219. The Unfair Competition Law, California Business & Professions Code §§
 22 17200, *et seq.* (the "UCL"), prohibits any "unlawful," "unfair," or "fraudulent" business
 23 act or practice, which can include false or misleading advertising.

24 220. Defendants violated, and continue to violate, the "unlawful" prong of the
 25 UCL through violation of statutes, constitutional provisions, and common law, as alleged
 26 herein.

27 221. Defendants violated, and continue to violate, the "unfair" prong of the UCL
 28 because they took private and personally-identifiable data and content – including the

1 User/Device Identifiers, the biometric identifiers and information, and the Private Videos
2 and Private Video Images never intended for public consumption – from the Plaintiffs’ and
3 the Class’s mobile devices and other social media accounts under circumstances in which
4 the Plaintiffs and the Class would have no reason to know that such data and content was
5 being taken.

6 222. The Plaintiffs and the Class had no reason to know because (i) there was no
7 disclosure of Defendants’ collection and transfer of the Plaintiffs’ and the Class’s
8 biometric identifiers and information, Private Videos and Private Video Images not
9 intended for public consumption; (ii) there was no disclosure of Defendants’ collection and
10 transfer of the Plaintiffs’ and the Class’s private and personally-identifiable data and
11 content before they even sign-up and create an account; (iii) there was no disclosure of
12 Defendants’ collection and transfer of the Plaintiffs’ and the Class’s private and
13 personally-identifiable data and content when the TikTok app is closed; (iv) there was no
14 disclosure that Defendants had embedded source code within the TikTok app that transfers
15 the Plaintiffs’ and the Class’s private and personally-identifiable data and content to
16 servers and third-party companies based in China where such servers and third-party
17 companies are subject to Chinese law requiring the sharing of such data and content with
18 the Chinese government; and (v) there was no effective disclosure of the wide range of the
19 private and personally-identifiable data and content, including User/Device Identifiers, that
20 Defendants took from the Plaintiffs’ and the Class’s mobile devices and other social media
21 accounts.

22 223. Defendants violated, and continue to violate, the “fraudulent” prong of the
23 UCL because (i) Defendants made it appear that the Plaintiffs’ and the Class’s
24 User/Device Identifiers, biometric identifiers and information, and Private Videos and
25 Private Video Images would not be collected and transferred unless the Plaintiffs and the
26 Class chose to do so, but in fact Defendants collected and transferred such data and content
27 without notice or consent; (ii) Defendants made it appear that the Plaintiffs’ and the
28 Class’s private and personally-identifiable data and content would not be collected and

1 transferred before they had signed-up and created an account, but in fact Defendants
2 collected and transferred such data and content before sign-up and account creation
3 without notice or consent; (iii) Defendants made it appear that the Plaintiffs' and the
4 Class's private and personally-identifiable data and content would not be collected or
5 transferred while the TikTok app is closed, but in fact Defendants clandestinely collected
6 and transferred such data and content when the app was closed without notice or consent;
7 (iv) Defendants made it appear that the Plaintiffs' and the Class's private and personally-
8 identifiable data and content would not be transferred to servers and third-party companies
9 based in China where such servers and third-party companies are subject to Chinese law
10 requiring the sharing of such data and content with the Chinese government, but in fact
11 Defendants covertly transferred such data and content to servers and third-party companies
12 based in China without notice or consent; and (v) Defendants have intentionally refrained
13 from disclosing the use to which the Plaintiffs' and the Class's private and personally-
14 identifiable data and content has been put, while simultaneously providing misleading
15 reassurances about Defendants' data collection and use practices. The Plaintiffs and the
16 Class were misled by Defendants' concealment, and had no reason to believe that
17 Defendants had taken the private and personally-identifiable data and content that they had
18 taken.

19 224. The Plaintiffs and the Class have been harmed and have suffered economic
20 injury as a result of Defendants' UCL violations. First, the Plaintiffs and the Class have
21 suffered harm in the form of diminution of the value of their private and personally-
22 identifiable data and content. Second, they have suffered harm to their mobile devices. The
23 battery, memory, CPU and bandwidth of such devices have been compromised, and as a
24 result the functioning of such devices has been impaired and slowed. Third, they have
25 incurred additional data usage and electricity costs that they would not otherwise have
26 incurred. Fourth, they have suffered harm as a result of the invasion of privacy stemming
27 from Defendants' covert theft of their private and personally-identifiable data and content
28 – including their User/Device Identifiers, biometric identifiers and information, and Private

1 Videos and Private Video Images.

2 225. Defendants, as a result of their conduct, have been able to reap unjust profits
3 and revenues in violation of the UCL. This includes Defendants' profits and revenues from
4 their targeted-advertising, improvements to their artificial intelligence technologies, their
5 patent applications, and the increased consumer demand for and use of Defendants' other
6 products. The Plaintiffs and the Class seek restitution and disgorgement of these unjust
7 profits and revenues.

8 226. Unless restrained and enjoined, Defendants will continue to misrepresent
9 their private and personally-identifiable data and content collection and use practices, and
10 will not recall and destroy Plaintiffs' and the Class's wrongfully collected private and
11 personally-identifiable data and content. Accordingly, injunctive relief is appropriate.

12 **SIXTH CAUSE OF ACTION**

13 **Violation of the California False Advertising Law,**

14 **Bus. & Prof. C. §§ 17500 *et seq.***

15 **(On Behalf of the Plaintiffs and the Class)**

16 227. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if
17 fully set forth herein.

18 228. California's False Advertising Law (the "FAL") – Cal. Bus. & Prof. Code §§
19 17500, *et seq.* – prohibits "any statement" that is "untrue or misleading" and made "with
20 the intent directly or indirectly to dispose of" property or services.

21 229. Defendants' advertising is, and at all relevant times was, highly misleading.
22 Defendants do not disclose at all, or do not meaningfully disclose, the private and
23 personally-identifiable data and content – including the User/Device Identifiers, the
24 biometric identifiers and information, and the Private Videos and Private Video Images
25 never intended for public consumption – that they have collected and transferred from the
26 Plaintiffs' and the Class's mobile devices and other social media accounts. Defendants also
27 do not advertise that Defendants secretly take private and personally-identifiable data and
28 content from the Plaintiffs' and the Class's mobile devices before they even sign up and

1 create an account, or that Defendants covertly take private and personally-identifiable data
 2 and content from the Plaintiffs' and the Class's mobile devices even when the TikTok app
 3 is closed. Nor do Defendants disclose that the Plaintiffs' and the Class's private and
 4 personally-identifiable data and content has been made available to foreign entities,
 5 including foreign government entities. As United States Senator Josh Hawley said on
 6 November 18, 2019: "If your child uses TikTok, there's a chance the Chinese Communist
 7 Party knows where they are, what they look like, what their voices sound like, and what
 8 they're watching" . . . "That's a feature TikTok doesn't advertise."¹³⁵

9 230. Reasonable consumers, like the Plaintiffs and the Class, are – and at all
 10 relevant times were – likely to be misled by Defendants' misrepresentations. Reasonable
 11 consumers lack the means to verify Defendants' representations concerning their data and
 12 content collection and use practices, or to understand the fact or significance of
 13 Defendants' data and content collection and use practices.

14 231. The Plaintiffs and the Class have been harmed and have suffered economic
 15 injury as a result of Defendants' misrepresentations. First, they have suffered harm in the
 16 form of diminution of the value of their private and personally-identifiable data and
 17 content. Second, they have suffered harm to their mobile devices. The battery, memory,
 18 CPU and bandwidth of such devices have been compromised, and as a result the
 19 functioning of such devices has been impaired and slowed. Third, they have incurred
 20 additional data usage and electricity costs that they would not otherwise have incurred.
 21 Fourth, they have suffered harm as a result of the invasion of privacy stemming from
 22 Defendants' covert theft of their private and personally-identifiable data and content –
 23 including their User/Device Identifiers, biometric identifiers and information, and Private
 24 Videos and Private Video Images.

25 232. Defendants, as a result of their misrepresentations, have been able to reap
 26

27 ¹³⁵ [https://www.law360.com/articles/1220783/no-more-data-storage-in-china-gop-senator-s-bill-](https://www.law360.com/articles/1220783/no-more-data-storage-in-china-gop-senator-s-bill-says)
 28 [says](https://www.law360.com/articles/1220783/no-more-data-storage-in-china-gop-senator-s-bill-says).

1 unjust profits and revenues. This includes Defendants' profits and revenues from their
 2 targeted-advertising, improvements to their artificial intelligence technologies, their patent
 3 applications, and the increased consumer demand for and use of Defendants' other
 4 products. The Plaintiffs and the Class seek restitution and disgorgement of these unjust
 5 profits and revenues.

6 233. Unless restrained and enjoined, Defendants will continue to misrepresent
 7 their private and personally-identifiable data and content collection and use practices, and
 8 will not recall and destroy Plaintiffs' and the Class's wrongfully collected private and
 9 personally-identifiable data and content. Accordingly, injunctive relief is appropriate.

10 **SEVENTH CAUSE OF ACTION**

11 **Negligence**

12 **(On Behalf of the Plaintiffs and the Class)**

13 234. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if
 14 fully set forth herein.

15 235. The Plaintiffs and the Class entrusted Defendants with their private and
 16 personally-identifiable data and content – including the User/Device Identifiers, the
 17 biometric identifiers and information, and the Private Videos and Private Video Images
 18 never intended for public consumption. Defendants had a duty to handle that data and
 19 content with care due its sensitivity, and the expectation that such data and content would
 20 not be shared with third parties. This duty included Defendants' assurances that third-
 21 parties would not improperly collect or obtain such data and content, and Defendants'
 22 public statements, made in response to direct inquiries about the ability of China-based
 23 entities to access U.S. TikTok user data, that the Plaintiffs' and the Class's private and
 24 personally-identifiable data was not in fact subject to such access.

25 236. The Plaintiffs' and the Class's willingness to entrust Defendants with their
 26 private and personally-identifiable data and content was predicated on the understanding
 27 that Defendants would take appropriate measures to protect it. Defendants had a special
 28 relationship with the Plaintiffs and the Class as a result of being entrusted with their

1 private and personally-identifiable data and content, which provided an independent duty
2 of care.

3 237. Defendants knew that the Plaintiffs' and the Class's private and personally-
4 identifiable data and content had value, and Defendants have earned substantial revenues
5 and profits as a result of collecting and using such private and personally-identifiable data
6 and content. This includes Defendants' profits and revenues from their targeted-
7 advertising, improvements to their artificial intelligence technologies, their patent
8 applications, and the increased consumer demand for and use of Defendants' other
9 products.

10 238. Defendants failed to use reasonable care to safeguard the Plaintiffs' and the
11 Class's private and personally-identifiable data and content, giving third parties access to it
12 without taking precautions to protect the Plaintiffs and the Class. Indeed, Defendants took
13 no precautions at all, instead making the Plaintiffs' and the Class's private and personally-
14 identifiable data and content directly available to third parties in jurisdictions with
15 inadequate privacy protections, and in jurisdictions with inadequate constraints on
16 governmental use of private and personally-identifiable data and content.

17 239. Defendants' failure to use care in allowing access to the Plaintiffs' and the
18 Class's private and personally-identifiable data and content has caused foreseeable harm.
19 Private and personally-identifiable data and content that can be used to track the physical
20 movements and online activities of the Plaintiffs and the Class, and that is biometrically
21 unique to each of the Plaintiffs and the members of the Class, has been transmitted to
22 China-based companies, thereby exposing the Plaintiffs and the Class to a heightened,
23 imminent risk of misuse, fraud, identity theft, Chinese government surveillance, and
24 financial harm.

25 240. The Plaintiffs' and the Class's private and personally-identifiable data and
26 content Defendants negligently allowed third parties to access allows such data and content
27 to be aggregated with other data and content to identify, profile and target the Plaintiffs
28 and the Class. As such, it is reasonable for the Plaintiffs and the Class to obtain identity

1 protection and credit monitoring services, and to recover the cost of these services from
2 Defendants.

3 241. The injury to the Plaintiffs and the Class was a proximate, reasonably
4 foreseeable result of Defendants' breaches of duty.

5 242. Defendants' conduct also constitutes gross negligence due to their extreme
6 departure from ordinary standards of care, and their knowledge that they had failed to
7 secure the Plaintiffs' and the Class's private and personally-identifiable data and content.

8 **EIGHTH CAUSE OF ACTION**

9 **Restitution / Unjust Enrichment**

10 **(On Behalf of the Plaintiffs and the Class)**

11 243. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if
12 fully set forth herein.

13 244. The Plaintiffs and the Class have conferred substantial benefits on
14 Defendants by downloading and using the TikTok app. These include the Defendants'
15 collection and use of the Plaintiffs' and the Class's private and personally-identifiable data
16 and content – including their User/Device Identifiers, biometric identifiers and
17 information, and Private Videos and Private Video Images never intended for public
18 consumption. Such benefits also include the revenues and profits resulting from
19 Defendants' collection and use of such data and content for Defendants' targeted-
20 advertising, improvements to their artificial intelligence technologies, their patent
21 applications, and the increased consumer demand for and use of Defendants' other
22 products.

23 245. Defendants have knowingly and willingly accepted and enjoyed these
24 benefits.

25 246. Defendants either knew or should have known that the benefits rendered by
26 the Plaintiffs and the Class were given with the expectation that Defendants would not take
27 and use the Plaintiffs' and the Class's private and personally-identifiable data and content
28 that Defendants have taken and used without permission. For Defendants to retain the

1 aforementioned benefits under these circumstances is inequitable.

2 247. Through deliberate violation of the Plaintiffs' and the Class's privacy
3 interests, and statutory and constitutional rights, Defendants each reaped benefits that
4 resulted in each Defendant wrongfully receiving profits.

5 248. Equity demands disgorgement of Defendants' ill-gotten gains. Defendants
6 will be unjustly enriched unless they are ordered to disgorge those profits for the benefit of
7 the Plaintiffs and the Class.

8 249. As a direct and proximate result of Defendants' wrongful conduct and unjust
9 enrichment, the Plaintiffs and the Class are entitled to restitution from Defendants and
10 institution of a constructive trust disgorging all profits, benefits, and other compensation
11 obtained by Defendants through this inequitable conduct.

12 **NINTH CAUSE OF ACTION**

13 **Violation of Illinois's Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.***

14 **(On Behalf of the Illinois Plaintiffs and the Illinois Subclass)**

15 250. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if
16 fully set forth herein.

17 251. BIPA makes it unlawful for any private entity to, among other things,
18 "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a
19 customer's biometric identifiers or biometric information, unless it first: (1) informs the
20 subject . . . in writing that a biometric identifier or biometric information is being collected
21 or stored; (2) informs the subject . . . in writing of the specific purpose and length of term
22 for which a biometric identifier or biometric information is being collected, stored, and
23 used; and (3) receives a written release executed by the subject of the biometric identifier
24 or biometric information or the subject's legally authorized representative." 740 ILCS
25 14/15(b).

26 252. Plaintiff Meghan Smith is, and at all relevant times was, an adult and
27 resident of Illinois, and thus is, and at all relevant times was, a "person" and/or a
28 "customer" within the meaning of BIPA. 740 ILCS 14/15(b). Plaintiff C.W. and Plaintiff

1 I.W. are, and at all relevant times were, minors and residents of Illinois, and thus are, and
2 at all relevant times were, “persons” and/or “customers” as well. *Id.* Plaintiff C.W.’s and
3 Plaintiff I.W.’s mother and legal guardian, Mikhaila Woodall, is Plaintiff C.W.’s and
4 Plaintiff I.W.’s “legally authorized representative” within the meaning of BIPA, and
5 served in such capacity at all times relevant to this action. *Id.* Plaintiff R.P. is, and at all
6 relevant times was, a minor and resident of Illinois, and thus is, and at all relevant times
7 was, a “person” and/or “customer” as well. *Id.* Plaintiff R.P.’s mother and legal guardian,
8 Lynn Pavalon, is Plaintiff R.P.’s “legally authorized representative” within the meaning of
9 BIPA, and served in such capacity at all times relevant to this action. *Id.*

10 253. Each Defendant is, and at all relevant times was, a “corporation, limited
11 liability company, association, or other group, however organized,” and thus is, and at all
12 relevant times was, a “private entity” under the BIPA. 740 ILCS 14/10.

13 254. The Illinois Plaintiffs and the Illinois Subclass had their “biometric
14 identifiers,” including their face geometry scans and voiceprints, as well as their
15 “biometric information” collected, captured, received, or otherwise obtained by
16 Defendants as a result of the Illinois Plaintiffs’ and the Illinois Subclass’s use of the
17 TikTok app. 740 ILCS 14/10.

18 255. At all relevant times, Defendants systematically and surreptitiously collected,
19 captured, received or otherwise obtained the Illinois Plaintiffs’ and the Illinois Subclass’s
20 “biometric identifiers” and “biometric information” without first obtaining signed written
21 releases, as required by 740 ILCS 14/15(b)(3), from any of them or their “legally
22 authorized representatives.”

23 256. In fact, Defendants failed to properly inform the Illinois Plaintiffs and the
24 Illinois Subclass, or any of their parents, legal guardians, or other “legally authorized
25 representatives,” in writing (or in any other way) that the Illinois Plaintiffs’ and the Illinois
26 Subclass’s “biometric identifiers” and “biometric information” were being “collected or
27 stored” by Defendants. Nor did Defendants inform the Illinois Plaintiffs and the Illinois
28 Subclass, or any of their parents, legal guardians, or other “legally authorized

representatives,” in writing of the specific purpose and length of term for which the Illinois Plaintiffs’ and the Illinois Subclass’s “biometric identifiers” and “biometric information” were being “collected, stored and used” as required by 740 ILCS 14/15(b)(1)-(2).

257. BIPA also makes it unlawful for a private entity “in possession of a biometric identifier or biometric information” to “sell, lease, trade, or otherwise profit from a person’s or a customer’s biometric identifier or biometric information.” 740 ILCS 14/15(c).

258. Defendants are, and at all relevant times were, “in possession of” the Illinois Plaintiffs’ and the Illinois Subclass’s “biometric identifiers,” including but not limited to their face geometry scans and voiceprints, and “biometric information.” Defendants profited from such “biometric identifiers” and “biometric information” by using them for targeted advertising, improvements to Defendants’ artificial intelligence technologies, Defendants’ patent applications, and the generation of increased demand for and use of Defendants’ other products. 740 ILCS 14/15(c).

259. Finally, BIPA prohibits private entities “in possession of a biometric identifier or biometric information” from “disclos[ing], redisclos[ing], or otherwise disseminat[ing] a person’s or a customer’s biometric identifier or biometric information unless” any one of four enumerated conditions are met. 740 ILCS 14/15(d)(1)-(4). None of such conditions are met here.

260. Defendants disclose, redisclose and disseminate, and at all relevant times disclosed, redisclosed and disseminated, the Illinois Plaintiffs’ and the Illinois Subclass’s “biometric identifiers,” including but not limited to their face geometry scans and voiceprints, and “biometric information” without the consent of any of them or their “legally authorized representatives.” 740 ILCS 14/15(d)(1). Moreover, the disclosures and redisclosures did not “complete[] a financial transaction requested or authorized by” the Illinois Plaintiffs, the Illinois Subclass or any of their legally authorized representatives. 740 ILCS 14/15(d)(2). Nor are, or at any relevant times were, the disclosures and redisclosures “required by State or federal law or municipal ordinance.” 740 ILCS

1 14/15(d)(3). Finally, at no point in time were the disclosures ever “required pursuant to a
 2 valid warrant or subpoena issued by a court of competent jurisdiction.” 740 ILCS
 3 14/15(d)(4).

4 261. BIPA mandates that a private entity “in possession of biometric identifiers or
 5 biometric information” “develop a written policy, made available to the public,
 6 establishing a retention schedule and guidelines for permanently destroying biometric
 7 identifiers and biometric information when the initial purpose for collecting or obtaining
 8 such identifiers or information has been satisfied or within 3 years of the individual’s last
 9 interaction with the private entity, whichever occurs first.” 740 ILCS 14/15(a).

10 262. But Defendants do not publicly provide any written policy establishing any
 11 retention schedule or guidelines for permanently destroying the Illinois Plaintiffs’ and the
 12 Illinois Subclass’s “biometric identifiers” and “biometric information.” 740 ILCS 14/15(a).

13 263. BIPA also commands private entities “in possession of a biometric identifier
 14 or biometric information” to: (1) store, transmit, and protect from disclosure all biometric
 15 identifiers and biometric information using the reasonable standard of care within the
 16 private entity’s industry; and (2) store, transmit, and protect from disclosure all biometric
 17 identifiers and biometric information in a manner that is the same as or more protective
 18 than the manner in which the private entity stores, transmits and protects other confidential
 19 and sensitive information. 740 ILCS 14/15(e). Based on the facts alleged herein, including
 20 Defendants’ lack of a public written policy, their failure to inform TikTok users that
 21 Defendants obtain such users’ “biometric identifiers” and “biometric information,” their
 22 failure to obtain written consent to collect or otherwise obtain TikTok users’ “biometric
 23 identifiers” and “biometric information,” and their unauthorized dissemination of TikTok
 24 users’ “biometric identifiers” and “biometric information,” Defendants have violated this
 25 provision too.

26 264. Defendants recklessly or intentionally violated each of BIPA’s requirements
 27 and infringed the Illinois Plaintiffs’ and the Illinois Subclass’s rights to keep their
 28 immutable and uniquely identifying biometric identifiers and biometric information

1 private. As individuals subjected to each of Defendants' BIPA violations above, the
2 Illinois Plaintiffs and the Illinois Subclass are and have been aggrieved. 740 ILCS 14/20.

3 265. On behalf of themselves and the Illinois Subclass, the Illinois Plaintiffs seek:
4 (1) injunctive and equitable relief as is necessary to protect the interests of the Illinois
5 Plaintiffs and the Illinois Subclass by requiring Defendants to comply with BIPA's
6 requirements; (2) \$1,000.00 or actual damages, whichever is greater, for each negligent
7 violation of BIPA by Defendants; (3) \$5,000.00 or actual damages, whichever is greater,
8 for each intentional or reckless violation of BIPA by Defendants; and (4) reasonable
9 attorneys' fees and costs, including expert witness fees and other litigation expenses. 740
10 ILCS 14/20(1)-(4).

11 **XII. PRAYER FOR RELIEF.**

12 WHEREFORE, Plaintiff respectfully requests relief against Defendants as set forth
13 below:

14 (a) entry of an order certifying the proposed Class and Subclasses pursuant to
15 Federal Rule of Civil Procedure 23;

16 (b) entry of an order appointing Plaintiffs as representatives of the Class and
17 Subclasses;

18 (c) entry of an order appointing Plaintiffs' counsel as co-lead counsel for the Class
19 and Subclasses;

20 (d) entry of an order for injunctive and declaratory relief as described herein,
21 including but not limited to:

22 (i) enjoining Defendants, their affiliates, associates, officers, employees
23 and agents from transmitting TikTok user data and content to China, to other locations or
24 facilities where such TikTok user data and content is accessible from within China, and/or
25 to anyone outside the defendant companies;

26 (ii) enjoining Defendants, their affiliates, associates, officers, employees
27 and agents from taking TikTok users' private draft videos (including any frames, digital
28 images or other content from such videos) and biometric identifiers and information

1 without advanced notice to, and the prior written consent of, such TikTok users or their
2 legally authorized representatives (and, for the Illinois Subclass, without being in
3 compliance with BIPA);

4 (iii) enjoining Defendants, their affiliates, associates, officers, employees
5 and agents from taking physical/digital location tracking data, device ID data, personally-
6 identifiable data and any other TikTok user data and content except that for which
7 appropriate notice and consent is provided and which Defendants can show to be
8 reasonably necessary for the lawful operation of the TikTok app within the United States;

9 (iv) mandating that Defendants, their affiliates, associates, officers,
10 employees and agents recall and destroy the TikTok user data and content already taken in
11 violation of law;

12 (v) mandating that Defendants, their affiliates, associates, officers,
13 employees and agents remove from the TikTok app all SDKs based in China or whose data
14 is otherwise accessible from within China;

15 (vi) mandating that Defendants, their affiliates, associates, officers,
16 employees and agents implement protocols to ensure that no TikTok user data and content
17 is transmitted to, or otherwise accessible from within, China;

18 (vii) mandating that Defendants, their affiliates, associates, officers,
19 employees and agents hire third-party monitors for a period of at least three years to ensure
20 that all of the above steps have been taken; and

21 (viii) mandating that Defendants, their affiliates, associates, officers,
22 employees and agents provide written verifications on a quarterly basis to the court and
23 counsel for the Plaintiffs in the form of a declaration under oath that the above steps have
24 been satisfied.

25 (e) entry of judgment in favor of each Class and Subclass member for damages
26 suffered as a result of the conduct alleged herein, punitive damages, restitution, and
27 disgorgement, to include interest and prejudgment interest;

28 (f) award Plaintiff reasonable attorneys' fees and costs; and

1 (g) grant such other and further legal and equitable relief as the court deems just and
2 equitable.

3 **XIII. DEMAND FOR JURY TRIAL.**

4 Plaintiffs demand a trial by jury on all issues so triable.

5
6 DATED: May 11, 2020

Ekwan E. Rhow - State Bar No. 174604
Dorothy Wolpert - State Bar No. 73213
Thomas R. Freeman - State Bar No. 135392
Marc E. Masters - State Bar No. 208375
BIRD, MARELLA, BOXER, WOLPERT,
NESSIM, DROOKS, LINCENBERG &
RHOW, P.C.
1875 Century Park East, 23rd Floor
Los Angeles, California 90067-2561
Telephone: (310) 201-2100
Facsimile: (310) 201-2110

13 By: /s/ Marc E. Masters

14 Marc E. Masters

15 *Attorneys for Plaintiffs Misty Hong, minor*
16 *A.S., through her mother and legal guardian*
17 *Laurel Slothower, and minor A.R., through her*
18 *mother and legal guardian Gilda Avila*

1 DATED: May 11, 2020

Marc L. Godino – State Bar No. 182689
Jonathan M. Rotter – State Bar No. 234137
Pavithra Rajesh – State Bar No. 323055
GLANCY PRONGAY & MURRAY LLP
1925 Century Park East, Suite 2100
Los Angeles, California 90067-2561
Telephone: (310) 201-9150
Email: info@glancylaw.com

6 By: /s/ Jonathan M. Rotter
Jonathan M. Rotter

8 *Attorneys for Plaintiffs Misty Hong, minor*
9 *A.S., through her mother and legal guardian*
10 *Laurel Slothower, and minor A.R., through her*
11 *mother and legal guardian Gilda Avila*

12 DATED: May 11, 2020

13 David M. Given – State Bar No. 142375
14 Nicholas A. Carlin – State Bar No. 112532
15 Brian S. Conlon – State Bar No. 303456
16 PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
17 39 Mesa Street, Suite 201
The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900
Email: dmg@phillaw.com

18 By: /s/ David M. Given
David M. Given

19 *Attorneys for Meghan Smith, minors C.W. and*
20 *I.W., through their mother and legal guardian*
21 *Mikhaila Woodall, and minor R.P., through*
22 *her mother and legal guardian Lynn Pavalon*

23 **ATTESTATION**

24 I, Jonathan M. Rotter, am the ECF user whose identification and password are being
25 used to file this document. In compliance with Local Rule 5-1(i)(3), I hereby attest that
26 each of the Signatories herein, concur in this filing.

27 DATED: May 11, 2020

s/ Jonathan M. Rotter
Jonathan M. Rotter

PROOF OF SERVICE BY ELECTRONIC POSTING

I, the undersigned say:

I am not a party to the above case and am over eighteen years old. On May 11, 2020, I served true and correct copies of the foregoing document, by posting the document electronically to the ECF website of the United States District Court for the Northern District of California, for receipt electronically by the parties listed on the Court's Service List.

I affirm under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on May 11, 2020, at Los Angeles, California.

s/ Jonathan M. Rotter

Jonathan M. Rotter